ZyAIR B-3000

802.11b Wireless Access Point

User's Guide

Version 3.50
8/2005

ZyXEL

Copyright

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.

Information for Canadian Users

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

Cet appareil numerique de la classe B est conforme a 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.

Safety Warnings

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

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

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.

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	
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	
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	
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		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
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		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 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		
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
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		

METHOD	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
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		
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 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 (0) 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

Safety Warnings 5

ZyXEL Limited Warranty 6

Customer Support.. 7

Preface 24

**Chapter 1
Getting to Know Your ZyAIR 26**

1.1 Introducing the ZyAIR 26
1.2 ZyAIR Features 26
1.2.1 Physical Features 26
1.2.2 Firmware Features 27
1.3 Applications for the ZyAIR 30
1.3.1 Access Point 31
1.3.2 Multiple ESS 31
1.3.3 AP + Bridge 32
1.3.4 Bridge / Repeater 33
1.3.5 Corporation Network Application 34

**Chapter 2
Hardware Installation and Initial Setup 36**

2.1 Front Panel of the ZyAIR 36
2.2 Top Panel and Connections of the ZyAIR 37
2.2.1 One 10/100M Ethernet Port 37
2.2.2 Power Port 38
2.2.3 The RESET Button 38
2.2.4 Antennas 38
2.3 Hardware Mounting Options 38
2.4 Additional Installation Requirements 39
2.5 Configuring Your ZyAIR 39

Chapter 3
Introducing the Web Configurator 40

3.1 Accessing the ZyAIR Web Configurator 40
3.2 Resetting the ZyAIR 41
3.2.1 .Procedure To Use The Reset Button 41
3.2.2 Method of Restoring Factory-Defaults 41
3.3 Navigating the ZyAIR Web Configurator 42

Chapter 4
Wizard Setup 44

4.1 Wizard Setup Overview 44
4.1.1 Channel 44
4.1.2 ESS ID 44
4.1.3 WEP Encryption 44
4.2 Wizard Setup: General Setup 45
4.3 Wizard Setup: Wireless LAN 45
4.4 Wizard Setup: IP Address 47
4.4.1 IP Address Assignment 47
4.4.2 IP Address and Subnet Mask 47
4.5 Basic Setup Complete 49

Chapter 5
System Screens 50

5.1 System Overview 50
5.2 Configuring General Setup 50
5.3 Configuring Password 51
5.4 Configuring Time Setting 52

Chapter 6
Wireless LAN 56

6.1 Introduction 56
6.2 Wireless Security Overview 56
6.2.1 Encryption 56
6.2.2 Authentication 56
6.2.3 Restricted Access 57
6.2.4 Hide ZyAIR Identity 57
6.2.5 Configuring Wireless LAN on the ZyAIR 57
6.2.6 WEP Encryption 58
6.3 Configuring the Wireless Screen 58
6.3.1 Access Point Mode 58
6.3.2 Multiple ESS Mode 61
6.3.3 Bridge/Repeater Mode 61
6.3.4 AP+Bridge Mode 64

6.4 Configuring Roaming 65
6.4.1 Requirements for Roaming 67
6.5 Layer-2 Isolation Introduction 68
6.6 Layer-2 Isolation Configuration 68
6.6.1 Layer-2 Isolation Examples 70
6.6.2 Layer-2 Isolation Example 1 70
6.6.3 Layer-2 Isolation Example 2 71
6.6.4 Layer-2 Isolation Example 3 72
6.7 MAC Filter 73
6.8 Introduction to WPA 75
6.8.1 WPA-PSK Application Example 75
6.8.2 WPA with RADIUS Application Example 75
6.8.3 Wireless Client WPA Supplicants 76
6.9 Configuring IEEE 802.1x and WPA 76
6.9.1 Authentication Required: 802.1x 77
6.9.2 Authentication Required : WPA 79
6.9.3 Authentication Required: WPA-PSK 80
6.10 Configuring Local User Database 81
6.11 Configuring RADIUS 82

Chapter 7
Multiple ESS and VLAN 86

7.1 Wireless LAN Infrastructures 86
7.1.1 Multiple ESS 86
7.1.2 Notes on Multiple-ESS 86
7.1.3 Multiple ESS Example 86
7.1.4 Multi-ESS with VLAN Example 87
7.1.5 Configuring Multiple ESS 87
7.1.5.1 Edit ESS 89
7.2 VLAN 90
7.2.1 VLAN Tagging 90
7.2.2 Second Rx VLAN ID 90
7.2.3 Management VLAN ID 92
7.2.4 Configuring VLAN 92
7.3 MAC Filter Summary 93

Chapter 8
IP Screen 94

8.1 Factory Ethernet Defaults 94
8.2 TCP/IP Parameters 94
8.2.1 IP Address and Subnet Mask 94
8.2.2 WAN IP Address Assignment 94
8.3 Configuring IP 95

Chapter 9
Log Screens 96

9.1 Configuring View Log 96
9.2 Configuring Log Settings 97

Chapter 10
Maintenance 100

10.1 Maintenance Overview 100
10.2 System Status Screen 100
10.2.1 System Statistics 101
10.3 Association List 101
10.4 Channel Usage 102
10.5 F/W Upload Screen 104
10.6 Configuration Screen 105
10.6.1 Backup Configuration 106
10.6.2 Restore Configuration 106
10.6.3 Back to Factory Defaults 107
10.7 Restart Screen 108

Chapter 11
Introducing the SMT 110

11.1 Connect to your ZyAIR Using Telnet 110
11.2 Changing the System Password 110
11.3 ZyAIR SMT Menus Overview 111
11.4 Navigating the SMT Interface 112
11.4.1 System Management Terminal Interface Summary 113

Chapter 12
General Setup 116

12.1 General Setup 116
12.1.1 Procedure To Configure Menu 1 116

Chapter 13
LAN Setup 118

13.1 LAN Setup 118
13.2 TCP/IP Ethernet Setup 118
13.3 Wireless LAN Setup 119
13.3.1 Configuring MAC Address Filter 121
13.3.2 Configuring Roaming 123

Chapter 14
Dial-in User Setup 126

14.1 Dial-in User Setup 126

Chapter 15
SNMP Configuration 128

15.1 About SNMP 128
15.2 Supported MIBs 129
15.3 SNMP Configuration 129
15.4 SNMP Traps 130

Chapter 16
System Security 132

16.1 System Security 132
16.1.1 System Password 132
16.1.2 Configuring External RADIUS Server 132
16.1.3 802.1x 134

Chapter 17
System Information and Diagnosis 138

17.1 System Status 138
17.2 System Information 139
17.2.1 System Information 140
17.2.2 Console Port Speed 141
17.3 Log and Trace 141
17.3.1 Viewing Error Log 141
17.4 Diagnostic 142

Chapter 18
Firmware and Configuration File Maintenance 144

18.1 Filename Conventions 144
18.2 Backup Configuration 145
18.2.1 Backup Configuration Using FTP 145
18.2.2 Using the FTP command from the DOS Prompt 146
18.2.3 Backup Configuration Using TFTP 147
18.2.4 Example: TFTP Command 148
18.2.5 Backup Via Console Port 148
18.3 Restore Configuration 149
18.3.1 Restore Using FTP 150
18.4 Uploading Firmware and Configuration Files 150
18.4.1 Firmware Upload 151
18.4.2 Configuration File Upload 151
18.4.3 Using the FTP command from the DOS Prompt Example 152
18.4.4 TFTP File Upload 152
18.4.5 Example: TFTP Command 153
18.4.6 Uploading Via Console Port 153
18.4.7 Uploading Firmware File Via Console Port 153

18.4.8 Example Xmodem Firmware Upload Using HyperTerminal 154
18.4.9 Uploading Configuration File Via Console Port 154
18.4.10 Example Xmodem Configuration Upload Using HyperTerminal 155

Chapter 19
System Maintenance and Information 156

19.1 Command Interpreter Mode 156
19.1.1 CNM 157
19.1.2 Configuring Vantage CNM 157
19.1.3 Configuration Example 160
19.2 Time and Date Setting 161
19.2.1 Resetting the Time 163

Appendix A
Troubleshooting 164

Appendix B
Specifications 166

Appendix C
Power over Ethernet Specifications 168

Appendix D
Brute-Force Password Guessing Protection 170

Appendix E
Setting up Your Computer's IP Address 172

Appendix F
IP Address Assignment Conflicts 184

Appendix G
Wireless LANs 188

Appendix H
IP Subnetting 198

Appendix I
Command Interpreter 206

Appendix J
Log Descriptions 208

Appendix K
Indoor Installation Recommendations 212

Appendix L
Power Adaptor Specifications 214

List of Figures

Figure 1 PoE Installation Example 27
Figure 2 WDS Functionality Example 28
Figure 3 Access Point Application 31
Figure 4 Multiple ESS Application 32
Figure 5 AP+Bridge Application 33
Figure 6 Bridge Mode Application 34
Figure 7 Repeater Mode Application 34
Figure 8 Corporation Network Application 35
Figure 9 .ZyAIR Front Panel 36
Figure 10 ZyAIR Top Panel 37
Figure 11 Change Password Screen 40
Figure 12 The MAIN MENU Screen of the Web Configurator 42
Figure 13 Wizard 1 : General Setup 45
Figure 14 Wizard 2 : Wireless LAN Setup 46
Figure 15 Wizard 3 : IP Address Assignment 48
Figure 16 Wizard 4 : Setup Complete 49
Figure 17 System General Setup 50
Figure 18 Password. 51
Figure 19 Time Setting 53
Figure 20 Wireless: Access Point 59
Figure 21 Bridging Example 61
Figure 22 Bridge Loop: Two Bridges Connected to Hub 62
Figure 23 Bridge Loop: Bridge Connected to Wired LAN 62
Figure 24 Wireless: Bridge/Repeater 63
Figure 25 Wireless : AP+Bridge 65
Figure 26 Roaming Example 66
Figure 27 Roaming 67
Figure 28 Layer-2 Isolation Application 68
Figure 29 Layer-2 Isolation Configuration Screen 69
Figure 30 Layer-2 Isolation Example 70
Figure 31 Layer-2 Isolation Example 1 71
Figure 32 Layer-2 Isolation Example 2 72
Figure 33 Layer-2 Isolation Example 3 72
Figure 34 MAC Address Filter 74
Figure 35 WPA - PSK Authentication 75
Figure 36 WPA with RADIUS Application Example2 76

Figure 37 Wireless LAN : 802.1x/WPA 77
Figure 38 Wireless LAN : 802.1x/WPA for 802.1x Protocol 78
Figure 39 Wireless LAN: 802.1x/WPA for WPA Protocol 80
Figure 40 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol 81
Figure 41 Local User Database 82
Figure 42 RADIUS 83
Figure 43 Multi-ESS with VLAN Example 87
Figure 44 Wireless : Multiple ESS 88
Figure 45 Wireless : Edit ESS 89
Figure 46 Second Rx VLAN ID Example 91
Figure 47 Edit ESS : Second Rx VLAN ID Example 91
Figure 48 ESS – VLAN ID and Second Rx VLAN ID Example 92
Figure 49 VLAN 92
Figure 50 MAC Filter Summary 93
Figure 51 IP Setup 95
Figure 52 View Log 97
Figure 53 Log Settings 98
Figure 54 System Status 100
Figure 55 System Status: Show Statistics 101
Figure 56 Association List 102
Figure 57 Channel Usage 103
Figure 58 Firmware Upload 104
Figure 59 Firmware Upload In Process 105
Figure 60 Network Temporarily Disconnecte 105
Figure 61 Firmware Upload Error 105
Figure 62 Configuration 106
Figure 63 Configuration Upload Successful 107
Figure 64 Network Temporarily Disconnected 107
Figure 65 Configuration Upload Error 107
Figure 66 Reset Warning Message 108
Figure 67 Restart Screen 108
Figure 68 Login Screen 110
Figure 69 Menu 23.1 System Security : Change Password 111
Figure 70 ZyAIR B-3000 SMT Main Menu 113
Figure 71 Menu 1 General Setup 117
Figure 72 Menu 3 LAN Setup 118
Figure 73 Menu 3.2 TCP/IP Setup 119
Figure 74 Menu 3.5 Wireless LAN Setup 120
Figure 75 Menu 3.5 Wireless LAN Setup 122
Figure 76 Menu 3.5.1 WLAN MAC Address Filter 123
Figure 77 Menu 3.5 Wireless LAN Setup 124
Figure 78 WLAN Roaming Configuration 124
Figure 79 Menu 14- Dial-in User Setup 126

Figure 80 Menu 14.1- Edit Dial-in User 127
Figure 81 SNMP Management Model 128
Figure 82 Menu 22 SNMP Configuration 130
Figure 83 Menu 23 System Security 132
Figure 84 Menu 23 System Security 133
Figure 85 Menu 23.2 System Security : RADIUS Server 133
Figure 86 Menu 23 System Security 134
Figure 87 Menu 23.4 System Security : IEEE802.1x 135
Figure 88 Menu 24 System Maintenance 138
Figure 89 Menu 24.1 System Maintenance : Status 139
Figure 90 Menu 24.2 System Information and Console Port Speed 140
Figure 91 Menu 24.2.1 System Information : Information 140
Figure 92 Menu 24.2.2 System Maintenance : Change Console Port Speed 141
Figure 93 Menu 24.3 System Maintenance : Log and Trace 142
Figure 94 Sample Error and Information Messages 142
Figure 95 Menu 24.4 System Maintenance : Diagnostic 142
Figure 96 Menu 24.5 Backup Configuration 146
Figure 97 FTP Session Example 147
Figure 98 System Maintenance: Backup Configuration 149
Figure 99 System Maintenance: Starting Xmodem Download Screen 149
Figure 100 Backup Configuration Example 149
Figure 101 Successful Backup Confirmation Screen 149
Figure 102 Menu 24.6 Restore Configuration 150
Figure 103 Menu 24.7 System Maintenance: Upload Firmware 150
Figure 104 Menu 24.7.1 System Maintenance : Upload System Firmware 151
Figure 105 Menu 24.7.2 System Maintenance: Upload System Configuration File 151
Figure 106 FTP Session Example 152
Figure 107 Menu 24.7.1 as seen using the Console Port 154
Figure 108 Example Xmodem Upload 154
Figure 109 Menu 24.7.2 as seen using the Console Port 155
Figure 110 Example Xmodem Upload 155
Figure 111 Menu 24 System Maintenance 157
Figure 112 Valid CI Commands 157
Figure 113 CNM CL 158
Figure 114 CNM Configuration Example 161
Figure 115 Menu 24.10 System Maintenance : Time and Date Setting 162
Figure 116 WIndows 95/98/Me: Network: Configuration 173
Figure 117 Windows 95/98/Me: TCP/IP Properties: IP Address 174
Figure 118 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 175
Figure 119 Windows XP: Start Menu 176
Figure 120 Windows XP: Control Panel 176
Figure 121 Windows XP: Control Panel: Network Connections: Properties 177
Figure 122 Windows XP: Local Area Connection Properties 177

Figure 123 Windows XP: Advanced TCP/IP Settings 178
Figure 124 Windows XP: Internet Protocol (TCP/IP) Properties 179
Figure 125 Macintosh OS 8/9: Apple Menu 180
Figure 126 Macintosh OS 8/9: TCP/IP 180
Figure 127 Macintosh OS X: Apple Menu 181
Figure 128 Macintosh OS X: Network 182
Figure 129 IP Address Conflicts: CaseA 184
Figure 130 IP Address Conflicts: Case B 185
Figure 131 IP Address Conflicts: Case C 185
Figure 132 IP Address Conflicts: Case D 186
Figure 133 Peer-to-Peer Communication in an Ad-hoc Network 188
Figure 134 Basic Service Set 189
Figure 135 Infrastructure WLAN 190
Figure 136 RTS/CTS 191

List of Tables

Table 1 Front Panel LED Description 37
Table 2 ZyAIR Wireless LAN Coverage 38
Table 3 Wizard 1 : General Setup 45
Table 4 Wizard 2 : Wireless LAN Setup 46
Table 5 Private IP Address Ranges 47
Table 6 Wizard 3 : IP Address Assignment 48
Table 7 System General Setup 50
Table 8 Password 51
Table 9 Time Setting 53
Table 10 ZyAIR Wireless Security Levels 58
Table 11 Wireless: Access Point 59
Table 12 Wireless: Bridge/Repeater 63
Table 13 Roaming 67
Table 14 Layer-2 Isolation Configuration 69
Table 15 MAC Address Filter 74
Table 16 Wireless LAN : 802.1x/WPA 77
Table 17 Wireless LAN : 802.1x/WPA for 802.1x Protocol 78
Table 18 Wireless LAN: 802.1x/WPA for WPA Protocol 80
Table 19 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol 81
Table 20 Local User Database 82
Table 21 RADIUS 83
Table 22 Wireless: Multiple ESS 88
Table 23 Wireless: Edit ESS 89
Table 24 VLAN 92
Table 25 MAC Filter Summary 93
Table 26 Private IP Address Ranges 94
Table 27 IP Setup 95
Table 28 View Log 97
Table 29 Log Settings 98
Table 30 System Status 100
Table 31 System Status: Show Statistics 101
Table 32 Association List 102
Table 33 Channel Usage 103
Table 34 Firmware Upload 104
Table 35 Restore Configuration 106
Table 36 SMT Menus Overview 111

Table 37 Main Menu Commands 112
Table 38 Main Menu Summary 113
Table 39 Menu 1 General Setup 117
Table 40 Menu 3.2 TCP/IP Setup 119
Table 41 Menu 3.5 Wireless LAN Setup 120
Table 42 Menu 3.5.1 WLAN MAC Address Filter 123
Table 43 Menu 3.5.4 Bridge Link Configuration 124
Table 44 Menu 14.1- Edit Dial-in User 127
Table 45 Menu 22 SNMP Configuration 130
Table 46 SNMP Traps 130
Table 47 Ports and Interface Types 131
Table 48 Menu 23.2 System Security : RADIUS Server 133
Table 49 Menu 23.4 System Security : IEEE802.1x 135
Table 50 Menu 24.1 System Maintenance : Status 139
Table 51 Menu 24.2.1 System Maintenance : Information 140
Table 52 Menu 24.4 System Maintenance Menu: Diagnostic 143
Table 53 Filename Conventions 145
Table 54 General Commands for Third Party FTP Clients 147
Table 55 General Commands for Third Party TFTP Clients 148
Table 56 CNM Commands 158
Table 57 System Maintenance : Time and Date Setting 162
Table 58 Troubleshooting the Start-Up of Your ZyAIR 164
Table 59 Troubleshooting the Ethernet Interface 164
Table 60 Troubleshooting the Password 165
Table 61 Troubleshooting Telnet 165
Table 62 Troubleshooting the WLAN Interface 165
Table 63 Hardware 166
Table 64 Firmware 166
Table 65 Power over Ethernet Injector Specifications 168
Table 66 Power over Ethernet Injector RJ-45 Port Pin Assignments 168
Table 67 Brute-Force Password Guessing Protection Commands 170
Table 68 IEEE 802.11b 192
Table 69 Comparison of EAP Authentication Types 196
Table 70 Wireless Security Relational Matrix 197
Table 71 Classes of IP Addresses 198
Table 72 Allowed IP Address Range By Class 199
Table 73 "Natural" Masks 199
Table 74 Alternative Subnet Mask Notation 200
Table 75 Two Subnets Example 200
Table 76 Subnet 1 201
Table 77 Subnet 2 201
Table 78 Subnet 1 202
Table 79 Subnet 2 202

Table 80 Subnet 3 202
Table 81 Subnet 4 203
Table 82 Eight Subnets 203
Table 83 Class C Subnet Planning 203
Table 84 Class B Subnet Planning 204
Table 85 System Maintenance Logs 208
Table 86 ICMP Notes 208
Table 87 Sys log 209
Table 88 Log Categories and Available Settings 210
Table 89 North American Plug Standards 214
Table 90 North American Plug Standards 214
Table 91 European Plug Standards 214
Table 92 United Kingdom Plug Standards 214
Table 93 Japan Plug Standards 214
Table 94 Australia and New Zealand Plug Standards 215

Preface

Congratulations on your purchase of the ZyAIR B-3000 - 802.11b wireless access point.

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

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.

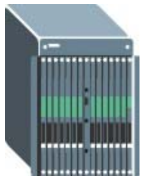
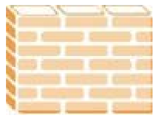
User Guide Feedback

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

The ZyAIR incorporates the IEEE802.11b standard for high-speed wireless transmission.

Additionally, the ZyAIR offers highly secured wireless connectivity to your wired network with IEEE 802.1x, 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.

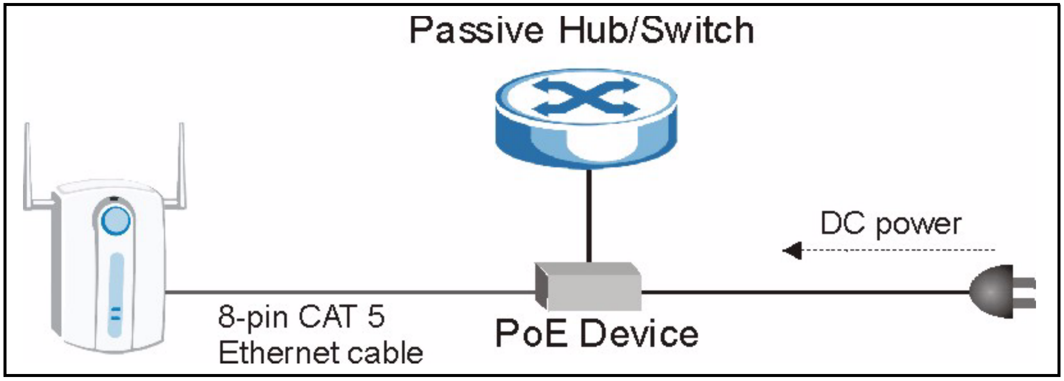
Bridge/Repeater LED

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

Multiple ESS

The ZyAIR's Multiple ESS (Multi-ESS) function allows multiple ESSs to be configured on just one access point (the ZyAIR). Different wireless stations can use different ESSIDs to associate with the same AP. Only wireless stations with the same ESSID can communicate with each other. This allows the AP to logically group wireless stations in a manner similar to VLAN (Virtual LAN).

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.

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.

VLAN

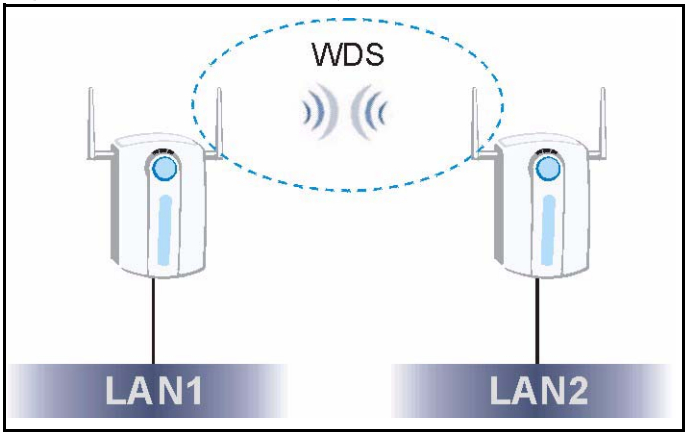
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can talk to each other. Stations on a logical network can belong to one or more groups. The ZyAIR supports 802.1Q VLAN tagging. Tagged VLAN uses an explicit 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.

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.

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 manger 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 application examples of what you can do with your ZyAIR.

The ZyAIR can be configured using the following WLAN operating modes

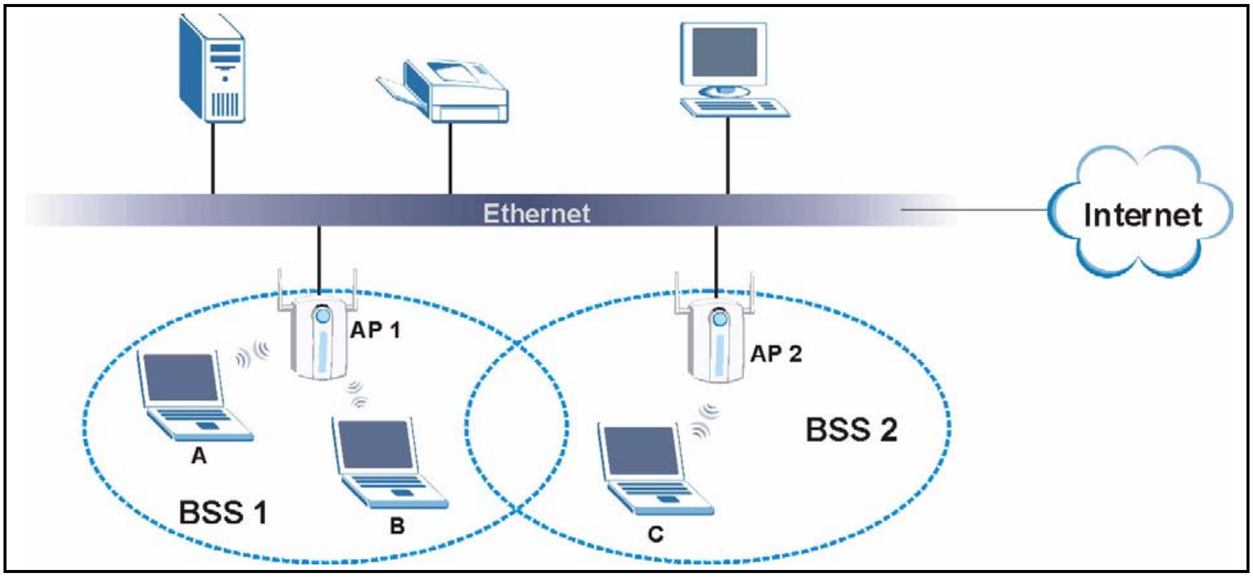
- AP
- Multiple ESS
- AP+Bridge
- Bridge/Repeater

Applications for each operating mode are shown below.

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

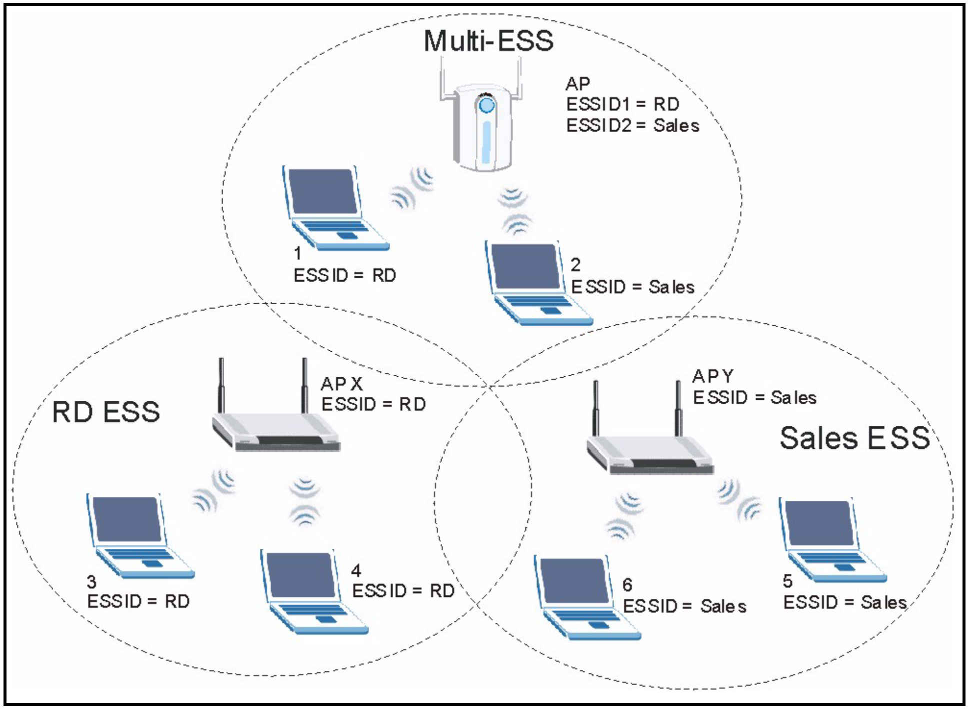
The ZyAIR's Multiple ESS function allows multiple ESSs to be configured on just one access point (the ZyAIR). Wireless stations can use different ESSIDs to associate with the same AP. Only wireless stations with the same ESSID can communicate with each other.

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

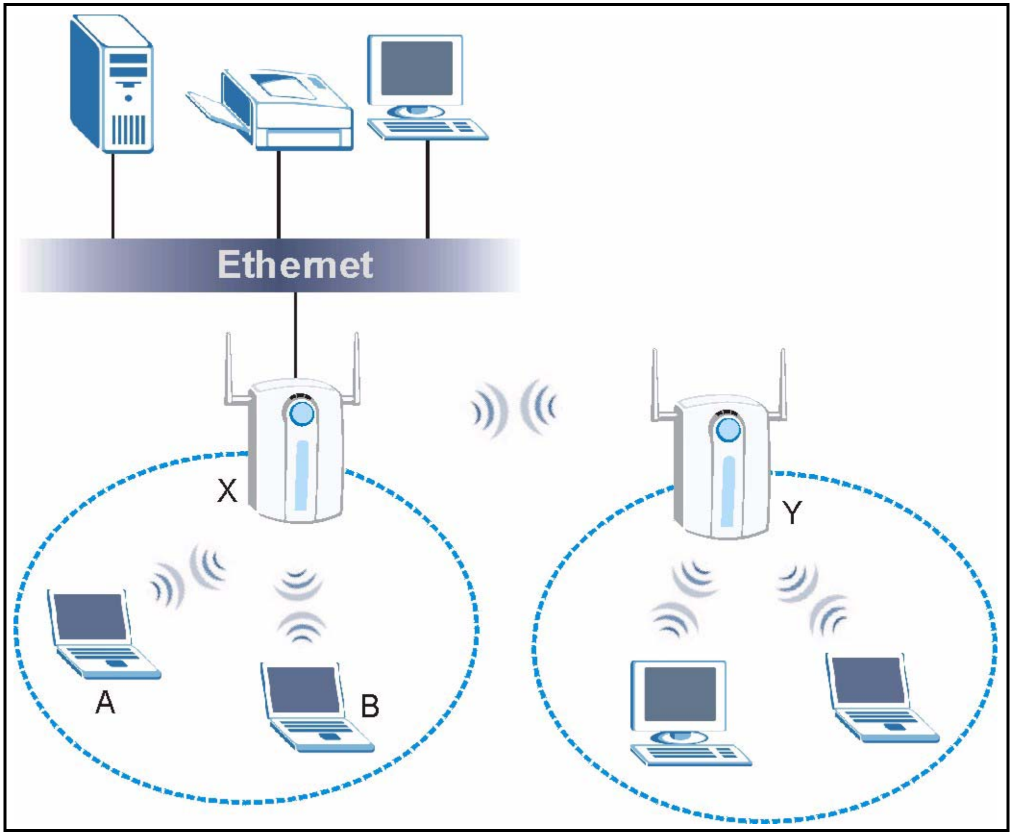


1.3.3 AP + Bridge

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 Mode Application

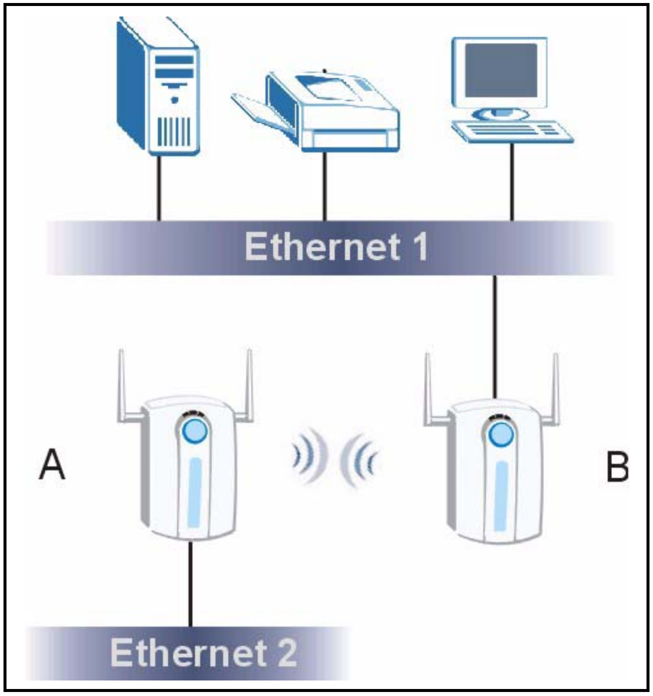
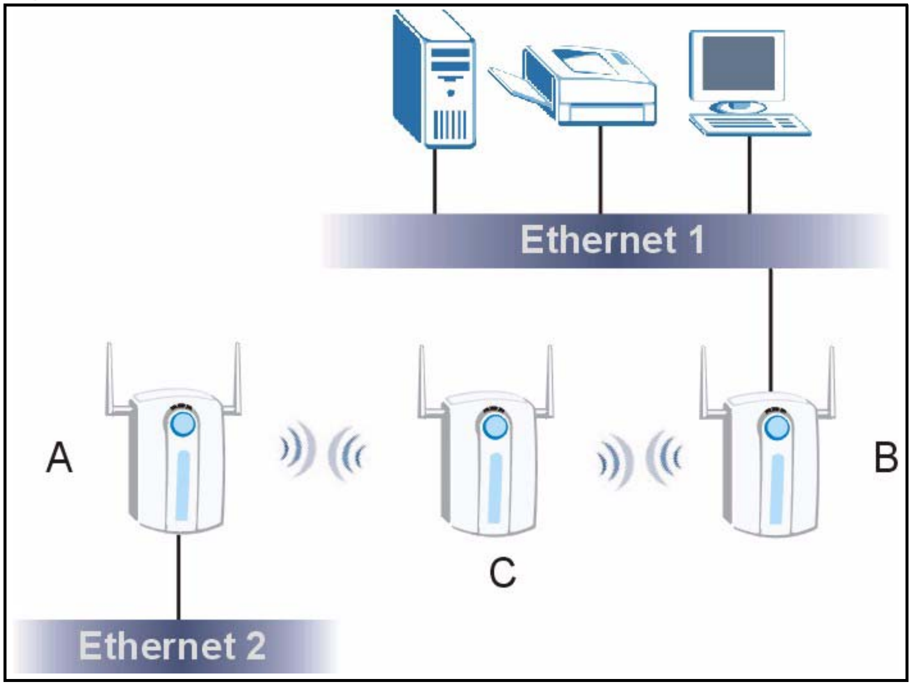


Figure 7 Repeater Mode Application

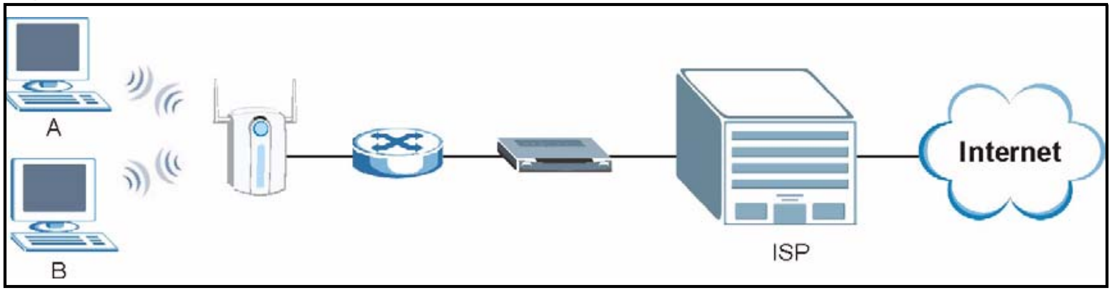


1.3.5 Corporation Network Application

In situations where users are always on the move in the coverage area but still need access to corporate network access, the ZyAIR is an ideal solution for wireless stations to connect to the corporate network without expensive network cabling.

The following figure depicts a typical application of the ZyAIR in an enterprise environment. Stations A and B with wireless adapters are allowed to access the network resource through the ZyAIR after account validation by the network authentication server.

Figure 8 Corporation Network Application



CHAPTER 2 Hardware Installation and Initial Setup

This chapter describes the physical features of the ZyAIR and how to make cable connections.

2.1 Front Panel of the ZyAIR

The LEDs on the front panel indicate the operational status of your ZyAIR.

Figure 9 .ZyAIR Front Panel

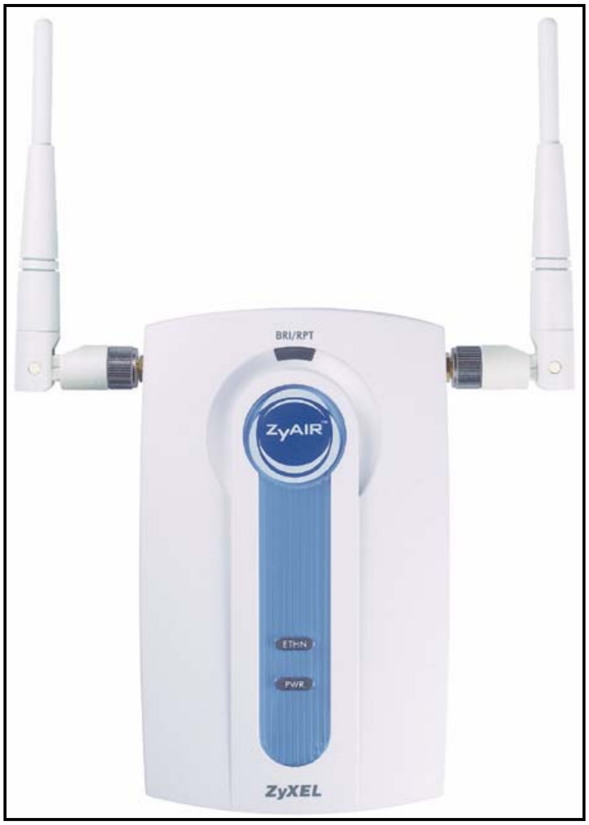


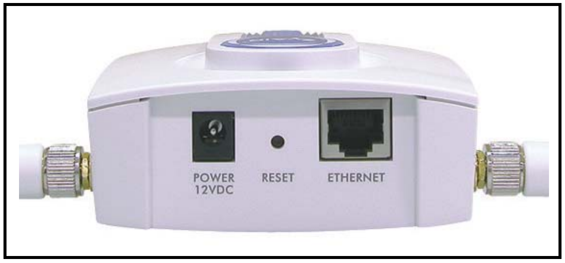
Table 1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
BRI/RPT	Green	On	The wireless card on the ZyAIR is working properly.
		Off	The wireless card on the ZyAIR is not ready or has a malfunction.
	Red	On	The ZyAIR is not ready or rebooting.
ZyAIR(WLAN ACK)	Blue	Breathing	The ZyAIR is sending or receiving data.
		On (dim)	The ZyAIR is ready, but is not sending or receiving data.
ETHN	Green	On	The ZyAIR has a successful 10Mb Ethernet connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have 10Mb Ethernet connection.
	Orange	On	The ZyAIR has a successful 100Mb Ethernet connection.
		Blinking	The ZyAIR is sending or receiving data.
		Off	The ZyAIR does not have 100Mb Ethernet connection.
PWR	Green	On	The ZyAIR is receiving power.
		Off	The ZyAIR is not receiving power.

2.2 Top Panel and Connections of the ZyAIR

The following figure shows the top panel of your ZyAIR.

Figure 10 ZyAIR Top Panel



2.2.1 One 10/100M Ethernet Port

Ethernet 10Base-T/100Base-T networks use Shielded Twisted Pair (STP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. The ETHERNET port is auto-sensing, so you may use the crossover cable provided or a straight-through Ethernet cable to connect your ZyAIR to a computer/external hub.

Note: When the ZyAIR is turned on and properly connected to a computer or a hub, the ETHN LED on the front panel turns on.

2.2.2 Power Port

Connect the power adapter to the port labeled POWER 12VDC on the top panel of your ZyAIR which then automatically turns on.

Note: The ZyAIR will reboot if the supplied power is too low. This is a normal operation.
Note: To avoid damage to the ZyAIR , make sure you use the supplied power adapter. Refer to the Power Adapter Specification appendix for more information.

2.2.3 The RESET Button

Hold this button in for about ten seconds (or until the Link LED turns red) to reboot and restore your ZyAIR to factory default values.

Note: All custom settings will be lost once you reset to the default settings.

2.2.4 Antennas

The ZyAIR is equipped with two reverse SMA connectors and two detachable omni-directional 2dBi antennas to provide clear radio signal between the wireless stations and the access points. Refer to the Antenna Selection and Positioning Recommendations appendix for more information.

The following table shows the ZyAIR's coverage (in meters) using the included antennas. The distance may differ depending on the network environment.

Table 2 ZyAIR Wireless LAN Coverage

	≤ **11 MBPS**	≤ **5.5 MBPS OR LOWER**
Indoor	50 m	80 m
Outdoor	200 m	300 m

Refer to the Quick Installation Guide for instructions on how to attach the antennas to the ZyAIR.

2.3 Hardware Mounting Options

The ZyAIR may be placed on a flat surface or wall mounted.

In general, the best place for the access point is at the center of your intended wireless coverage area. For better performance, mount the ZyAIR in a high position free of obstructions.

Refer to the Quick Start Guide for hardware mounting procedure.

2.4 Additional Installation Requirements

- A computer(s) with an installed network card or an IEEE 802.11b-compliant PCMCIA wireless LAN card.
- To enable remote RADIUS authentication for wireless clients, you need
  - A wireless client computer running IEEE 802.1x-compliant client software. Currently, this is bundled with Windows XP.
  - A network RADIUS server for remote user authentication and accounting.

2.5 Configuring Your ZyAIR

Configure your ZyAIR using:

- Web configurator
- SMT (System Management Terminal). Access the SMT using Telnet.

CHAPTER 3
Introducing the Web Configurator

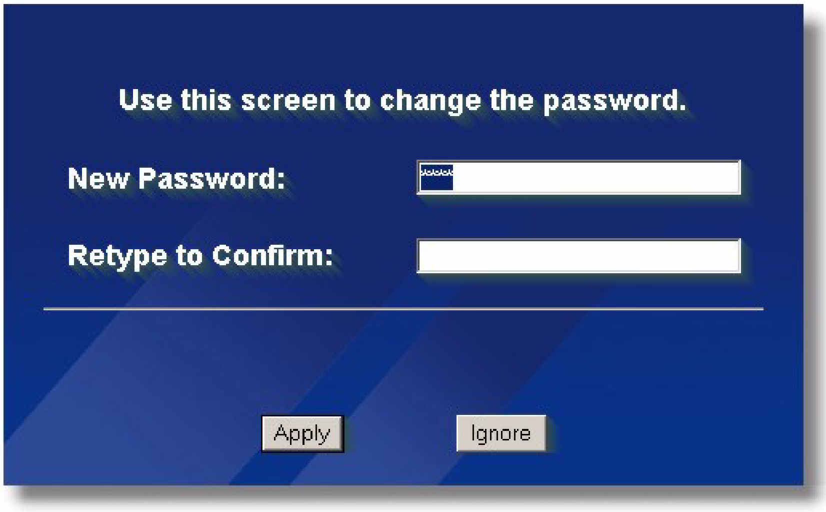
This chapter describes how to access the ZyAIR web configurator and provides an overview of its screens. The default IP address of the ZyAIR is 192.168.1.2.

3.1 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 11 Change Password Screen



Use this screen to change the password.

New Password: ****

Retype to Confirm:

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.

3.2 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.

3.2.1 .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.

3.2.2 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 10).

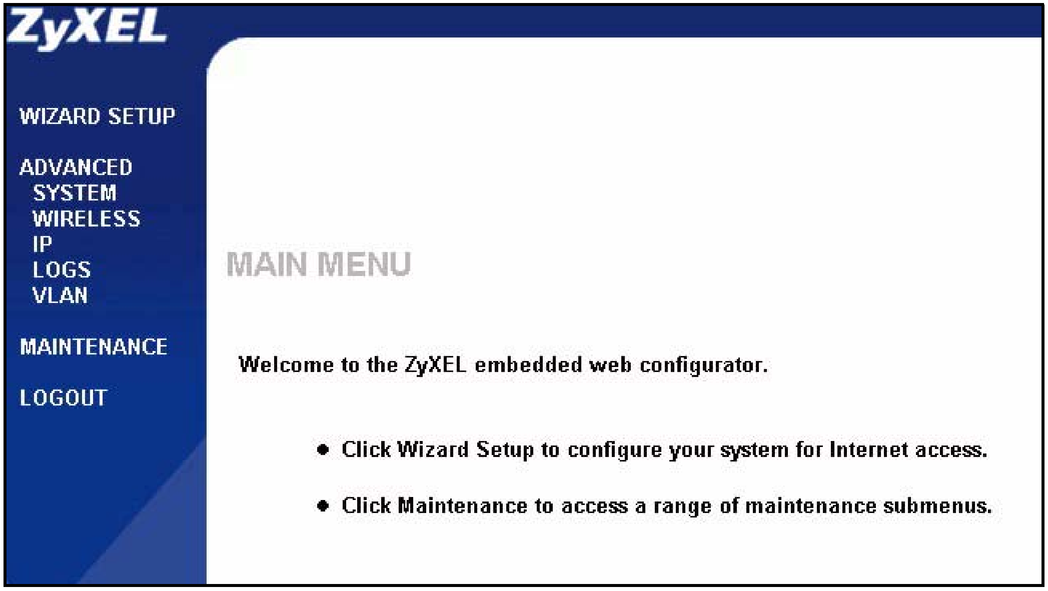
Transfer the configuration file to your ZyAIR using FTP. See later in the part on SMT configuration for more information.

3.3 Navigating the ZyAIR Web Configurator

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 HELP icon (located in the top right corner of most screens) to view online help.
Note: The HELP icon does not appear in the MAIN MENU screen.

Figure 12 The MAIN MENU Screen of the Web Configurator



MAIN MENU

Welcome to the ZyXEL embedded web configurator.

- Click Wizard Setup to configure your system for Internet access.
- Click Maintenance to access a range of maintenance submenus.

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, Layer-2 Isolation, MAC Filter, Roaming, 802.1x, Local User Database and RADIUS), **IP**, **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 4
Wizard Setup

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

4.1 Wizard Setup Overview

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

4.1.1 Channel

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

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

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

4.1.2 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.

4.1.3 WEP Encryption

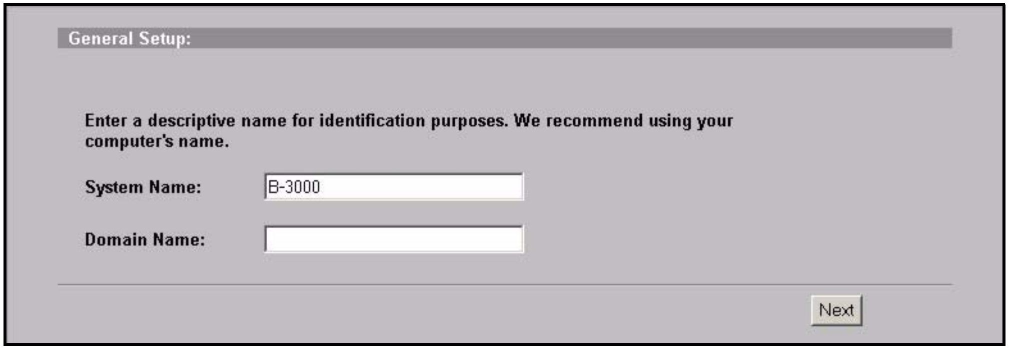
WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

4.2 Wizard Setup: General Setup

General Setup contains administrative and system-related information.

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

Figure 13 Wizard 1 : General Setup



General Setup:

Enter a descriptive name for identification purposes. We recommend using your computer's name.

System Name: B-3000

Domain Name:

The following table describes the labels in this screen.

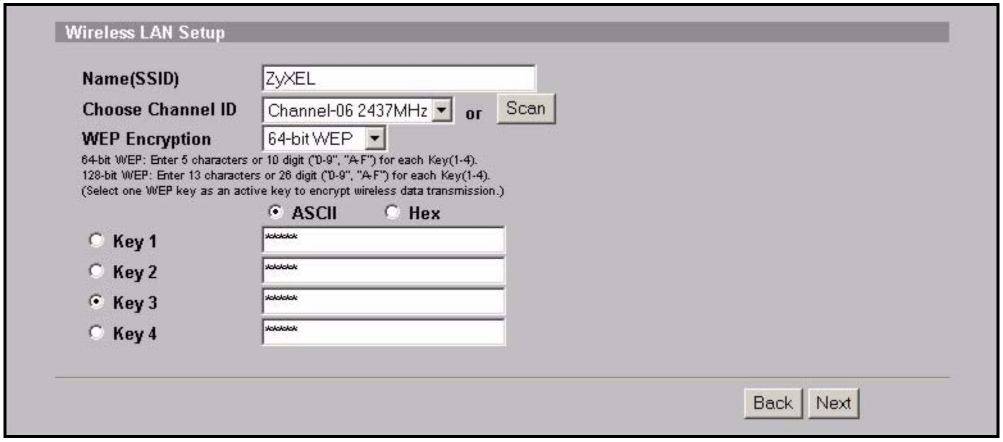
Table 3 Wizard 1 : General Setup

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.

4.3 Wizard Setup: Wireless LAN

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

Figure 14 Wizard 2 : Wireless LAN Setup



Wireless LAN Setup

Name(SSID): ZyXEL

Choose Channel ID: Channel-06 2437MHz or Scan

WEP Encryption: 64-bit WEP

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

○ Key 1: *****
○ Key 2: *****
● Key 3: *****
○ Key 4: *****

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.

4.4 Wizard Setup: IP Address

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

4.4.1 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.

4.4.2 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.

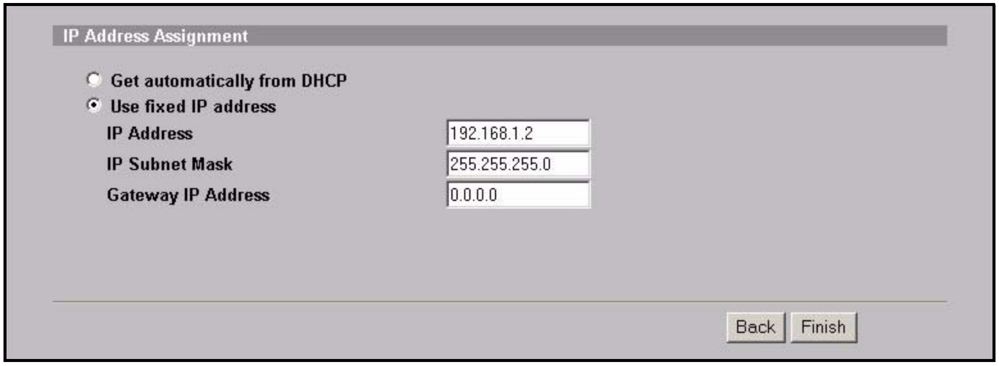
Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

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 15 Wizard 3 : IP Address Assignment



IP Address Assignment

○ Get automatically from DHCP

● Use fixed IP address

IP Address	192.168.1.2
IP Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0

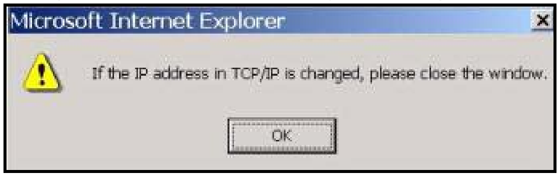
The following table describes the labels in this screen.

Table 6 Wizard 3 : IP Address Assignment

LABEL	DESCRIPTION
IP Address Assignment	
	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 neighbour 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.

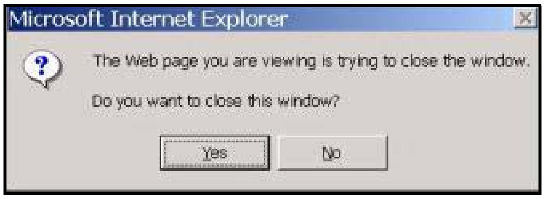
4.5 Basic Setup Complete

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).



If the IP address in TCP/IP is changed, please close the window.

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

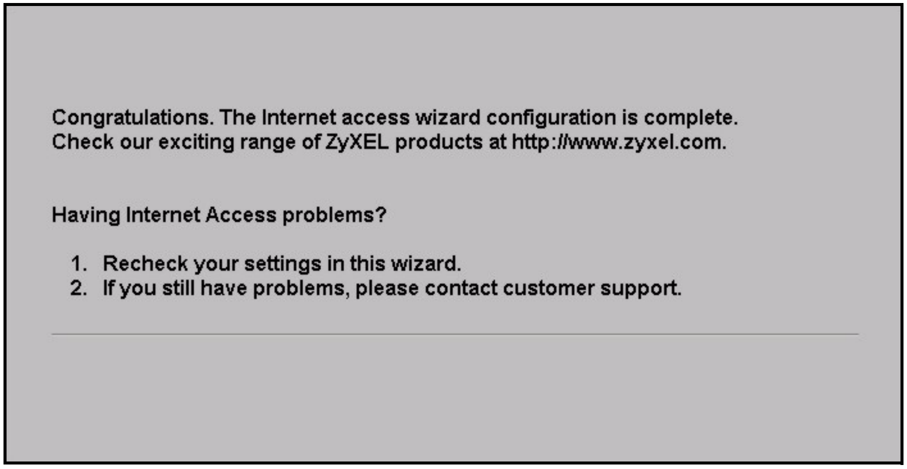


The Web page you are viewing is trying to close the window.

Do you want to close this window?

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

Figure 16 Wizard 4 : Setup Complete



Congratulations. The Internet access wizard configuration is complete.
Check our exciting range of ZyXEL products at http://www.zyxel.com.

Having Internet Access problems?

1. Recheck your settings in this wizard.
2. If you still have problems, please contact customer support.

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

CHAPTER 5
System Screens

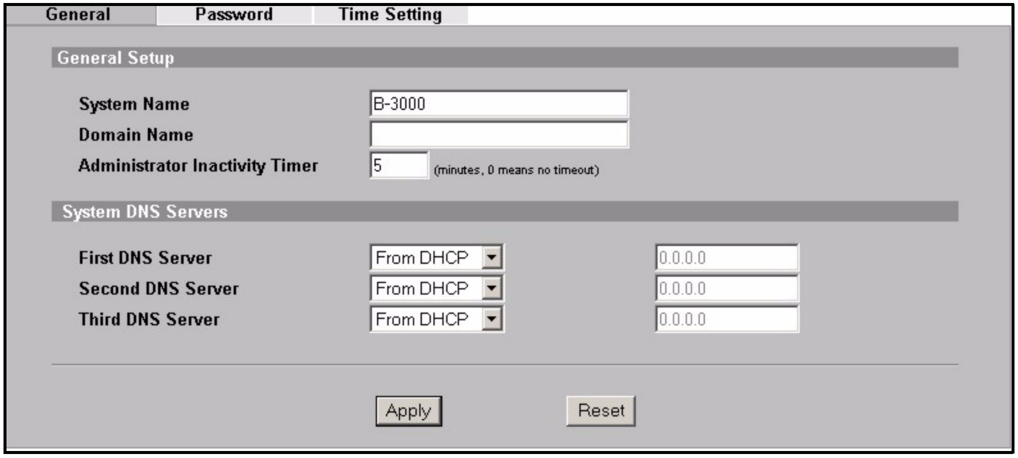
5.1 System Overview

This section provides information on general system setup.

5.2 Configuring General Setup

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

Figure 17 System General Setup



General Setup

System Name	B-3000	
Domain Name		
Administrator Inactivity Timer	5	(minutes, 0 means no timeout)

System DNS Servers

First DNS Server	From DHCP	0.0.0.0
Second DNS Server	From DHCP	0.0.0.0
Third DNS Server	From DHCP	0.0.0.0

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.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. 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. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).

Table 7 System General Setup

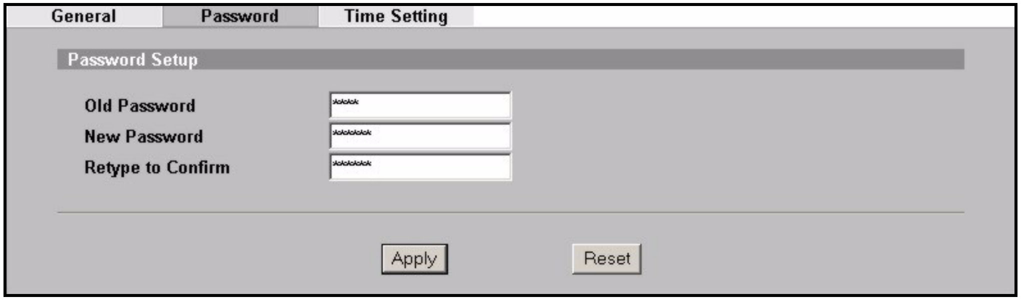
LABEL	DESCRIPTION
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From DHCP** if your DHCP server dynamically assigns DNS server information (and the ZyAIR's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. 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**. 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. The default setting is **None**.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.3 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 18 Password.



Old Password ****
New Password ******
Retype to Confirm ******

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.

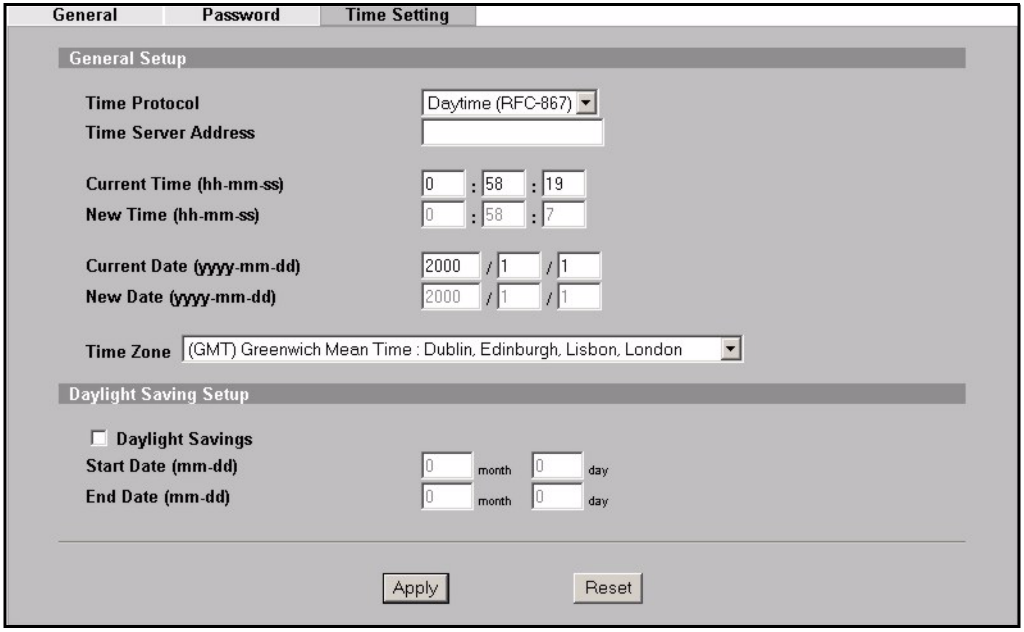
Table 8 Password

LABEL	DESCRIPTIONS
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.4 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 19 Time Setting



Time Protocol: Daytime (RFC-867)

Time Server Address:

Current Time (hh-mm-ss): 0 : 58 : 19

New Time (hh-mm-ss): 0 : 58 : 7

Current Date (yyyy-mm-dd): 2000 / 1 / 1

New Date (yyyy-mm-dd): 2000 / 1 / 1

Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Daylight Savings

Start Date (mm-dd): 0 month 0 day

End Date (mm-dd): 0 month 0 day

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 6 Wireless LAN

This chapter discusses how to configure Wireless LAN.

6.1 Introduction

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

Note: See the WLAN appendix for more detailed information on WLANs.

6.2 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.

6.2.1 Encryption

- Use WPA security if you have WPA-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK if you have WPA-aware wireless clients but no RADIUS server.
- If you don't have WPA-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can use Passphrase to automatically generate 64-bit or 128-bit WEP keys or manually enter 64-bit, 128-bit or 256-bit WEP keys.

6.2.2 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

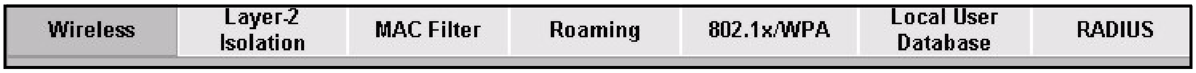
6.2.3 Restricted Access

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**).

6.2.4 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. If you don't hide the ESSID, at least you should change the default one.

6.2.5 Configuring Wireless LAN on the ZyAIR



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 configure **SSID** and **WEP** in the **Wireless** screen. If you configure **WEP**, you can't configure **WPA** or **WPA-PSK**.

2 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.

3 Use the **MAC Filter** screen to restrict access to your wireless network by MAC address.

4 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.

5 Configure **WPA** or **WPA-PSK** in the **802.1x/WPA** screen. Configure 802.1x wireless client authentication in the **802.1x/WPA** screen and the RADIUS authentication and accounting settings.

6 Configure the built-in authentication database in the **Local User Database** screen.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyAIR.

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

Table 10 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
Most Secure	Wi-Fi Protected Access (WPA)

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

6.2.6 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, 128-bit or 256-bit WEP keys but only one key can be enabled at any one time.

6.3 Configuring the Wireless Screen

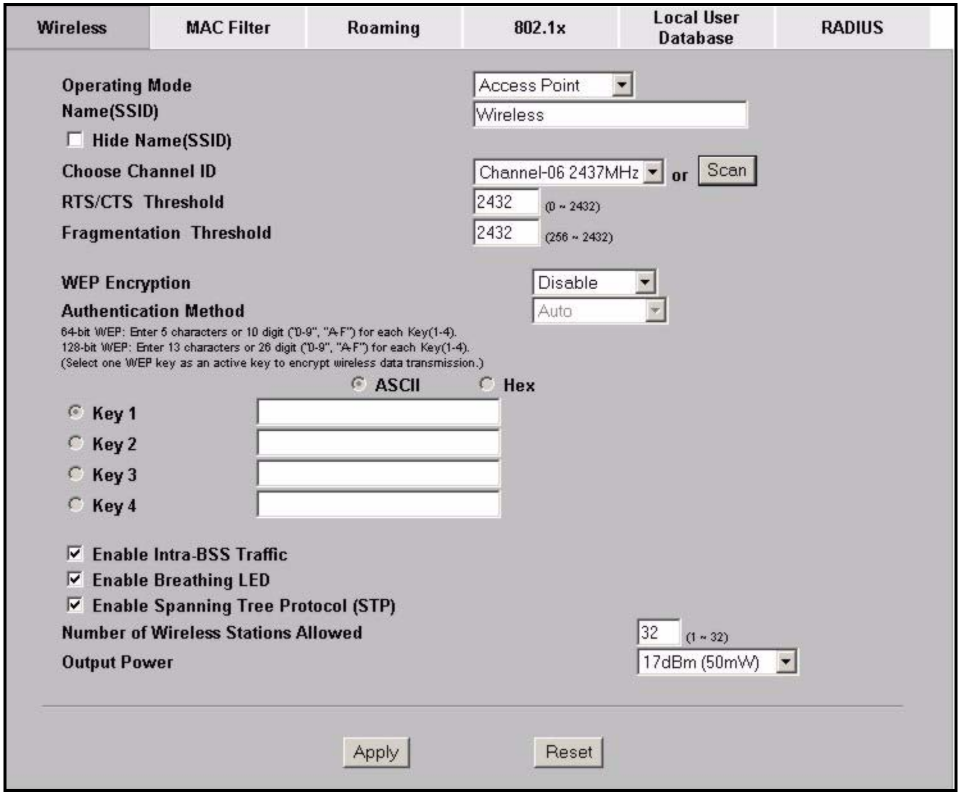
Click **WIRELESS** and then the **Wireless** tab to the display the **Wireless** screen.

The screen varies depending upon the operating mode you select.

6.3.1 Access Point Mode

Select **Access Point** from the **Operating Mode** drop-down list box in the following screen to display the screen as shown next.

Figure 20   Wireless: Access Point



Operating Mode: Access Point

Name(SSID): Wireless

□ Hide Name(SSID)

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

☑ Enable Intra-BSS Traffic
☑ Enable Breathing LED
☑ Enable Spanning Tree Protocol (STP)

Number of Wireless Stations Allowed: 32 (1 ~ 32)

Output Power: 17dBm (50mW)

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

Table 11   Wireless: Access Point

LABEL	DESCRIPTION
Operating Mode	Select the operating mode from the drop-down list. Options are Access Point, Multiple ESS, Bridge/Repeater and AP+Bridge. The screen changes when you select Multiple ESS, Bridge/Repeater or AP+Bridge in this field. Refer to the Multiple ESS and VLAN chapter for more information on multiple ESS.
Name (SSID)	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. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **Note:** If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's SSID or WEP 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.
Hide Name (SSID)	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool.

Table 11 Wireless: Access Point

LABEL	DESCRIPTION
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 **0** 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**.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. 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.
Key 1 to Key 4	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. 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. 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. 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.
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 Protocol (STP)	Select the check box to activate STP on the ZyAIR. (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.
Number of Wireless Stations Allowed	Use this field to set a maximum number of wireless stations that may connect to the ZyAIR. Enter the number (from 1 to 32) of wireless stations allowed.

Table 11 Wireless: Access Point

LABEL	DESCRIPTION
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)** or **11dBm (12.6mW)**.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

6.3.2 Multiple ESS Mode

Select **Multiple ESS** from the **Operating Mode** drop-down list box to display the following screen. Refer to the chapter on **Multiple ESS and VLAN** for configuration and detailed information.

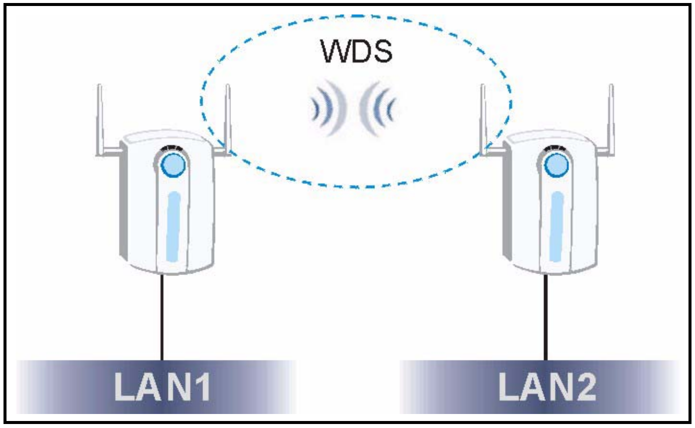
You cannot configure WPA on your ZyAIR in **Multiple ESS** mode.

6.3.3 Bridge/Repeater Mode

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

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.

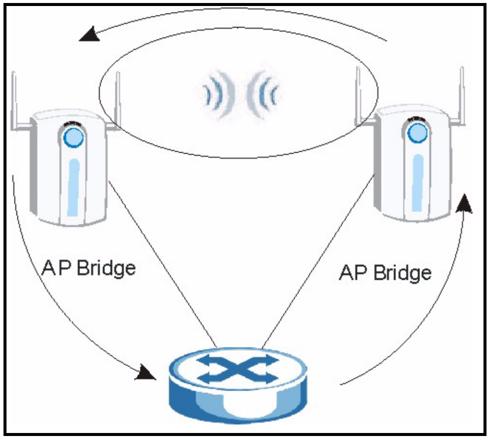
Figure 21 Bridging Example



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:

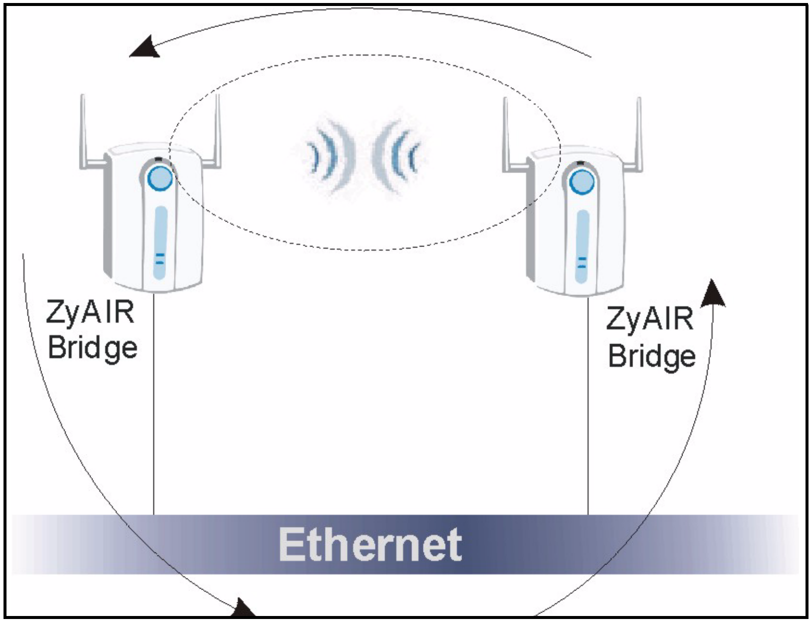
- If two or more ZyAIRs (in bridge mode) are connected to the same hub as shown next.

Figure 22 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.

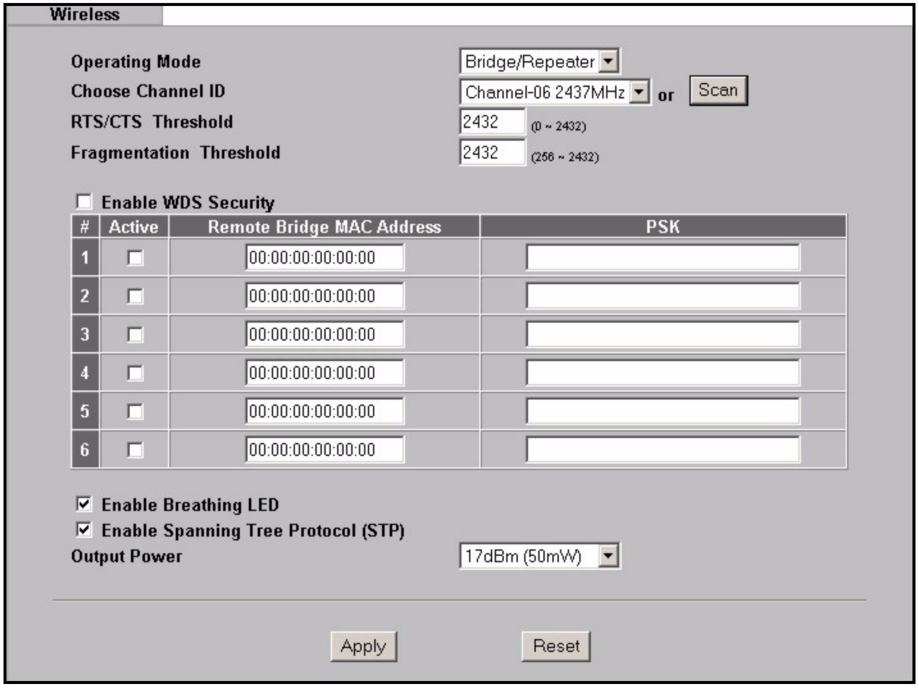
Figure 23 Bridge Loop: Bridge Connected to Wired LAN



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** from the **Operating Mode** drop-down list box to have the ZyAIR act as a wireless bridge only.

Figure 24 Wireless: Bridge/Repeater



Operating Mode: Bridge/Repeater

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

☐ Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	☐	00:00:00:00:00:00	
2	☐	00:00:00:00:00:00	
3	☐	00:00:00:00:00:00	
4	☐	00:00:00:00:00:00	
5	☐	00:00:00:00:00:00	
6	☐	00:00:00:00:00:00	

☑ Enable Breathing LED

☑ Enable Spanning Tree Protocol (STP)

Output Power: 17dBm (50mW)

The following table describes the bridge labels in this screen.

Table 12 Wireless: Bridge/Repeater

LABEL	DESCRIPTION
Operating Mode	Select Bridge/Repeater in this field to display the screen as shown
Enable WDS Security	Select the check box to encrypt traffic on the Wireless Distribution System (WDS). A 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. **Note:** Other AP's with WDS enabled must use TKIP encryption with the same PSK.
#	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).
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.

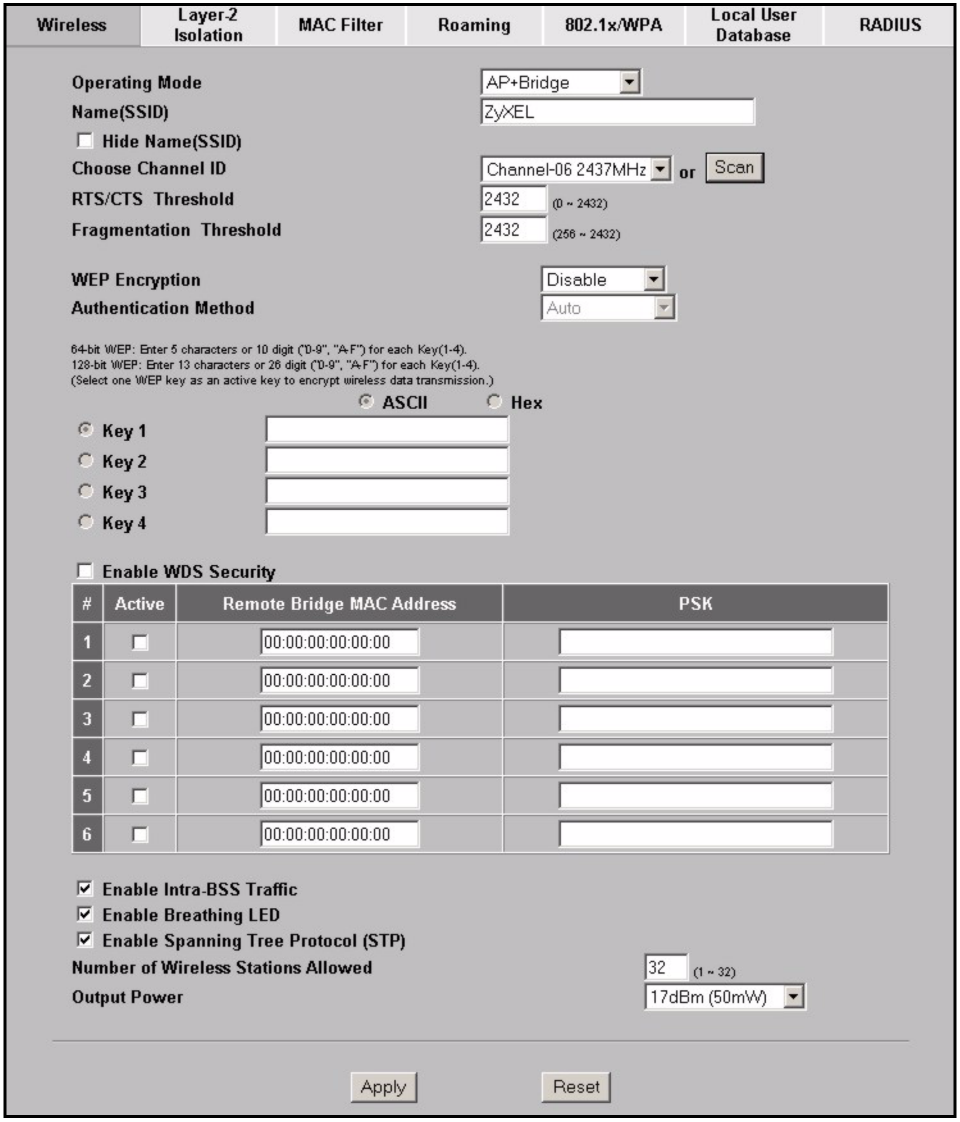
Table 12 Wireless: Bridge/Repeater

LABEL	DESCRIPTION
Enable Spanning Tree Protocol (STP)	Select the check box to activate STP on the ZyAIR.(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. The options are **17dBm (50mW)**, **15dBm (32mW)**, **13dBm (20mW)** or **11dBm (12.6mW)**.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

6.3.4 AP+Bridge Mode

Click the **WIRELESS** link under **ADVANCED**. Select **AP+Bridge** in the **Operating Mode** drop-down list box 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 25 Wireless : AP+Bridge



Operating Mode	AP+Bridge
Name(SSID)	ZyXEL
□ Hide Name(SSID)	
Choose Channel ID	Channel-06 2437MHz or Scan
RTS/CTS Threshold	2432 (0 ~ 2432)
Fragmentation Threshold	2432 (256 ~ 2432)
WEP Encryption	Disable
Authentication Method	Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

□ Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	□	00:00:00:00:00:00	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	
6	□	00:00:00:00:00:00	

☑ Enable Intra-BSS Traffic
☑ Enable Breathing LED
☑ Enable Spanning Tree Protocol (STP)

Number of Wireless Stations Allowed	32 (1 ~ 32)
Output Power	17dBm (50mW)

6.4 Configuring Roaming

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

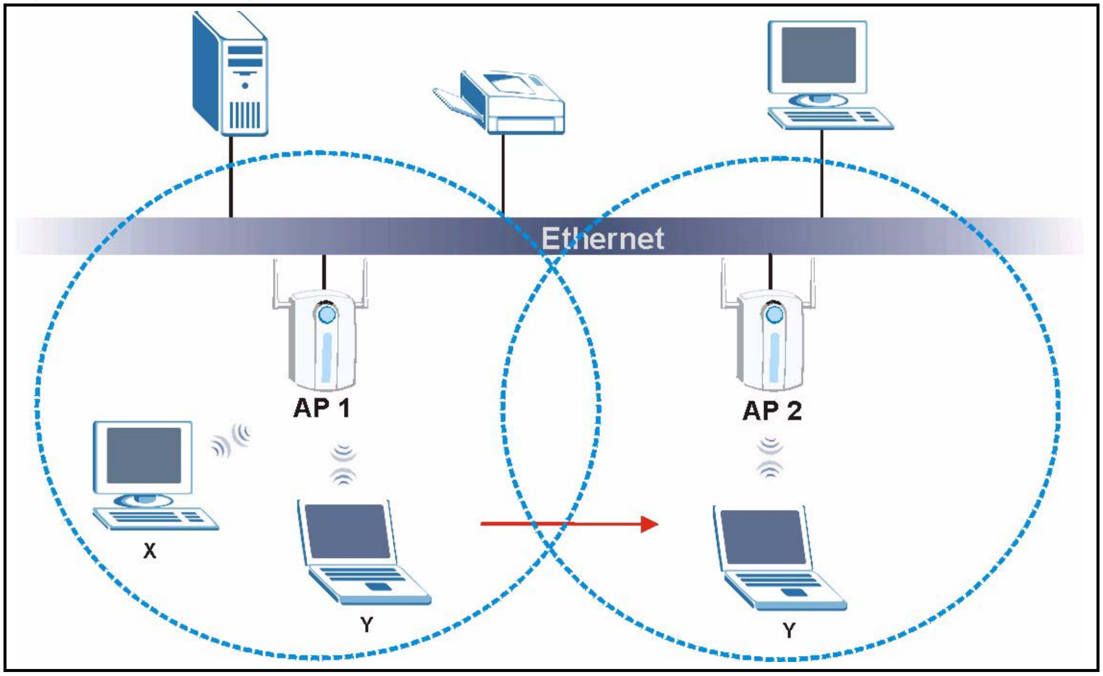
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending 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 26.

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 26 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.

6.4.1 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.

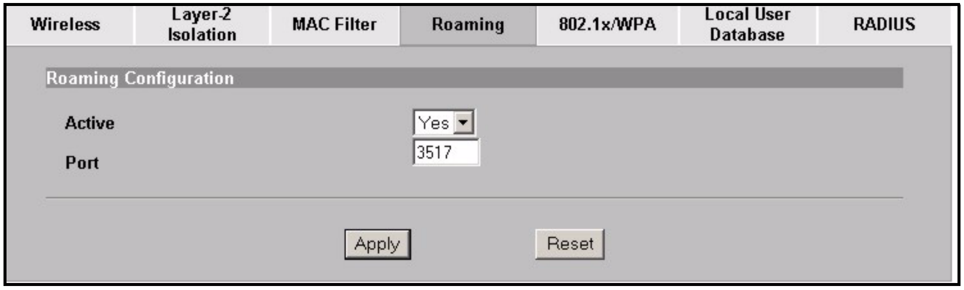
3 The adjacent access points should use different radio channels when their coverage areas overlap.

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 27 Roaming



Roaming Configuration

Active: Yes

Port: 3517

The following table describes the labels in this screen.

Table 13 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.

6.5 Layer-2 Isolation Introduction

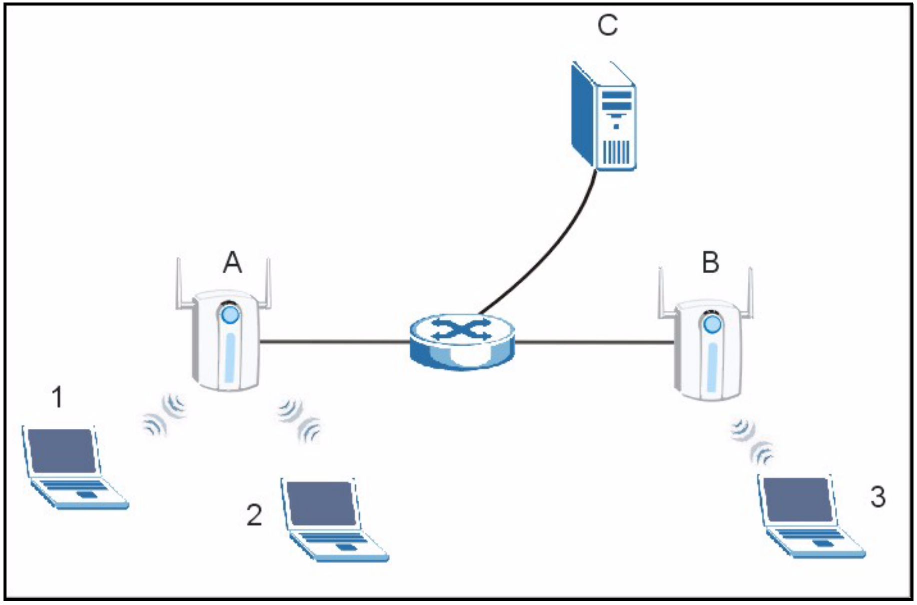
Layer-2 isolation is used to prevent wireless clients associated with your ZyAIR from communicating with other wireless clients, AP's, computers or routers in a network.

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 28 Layer-2 Isolation Application



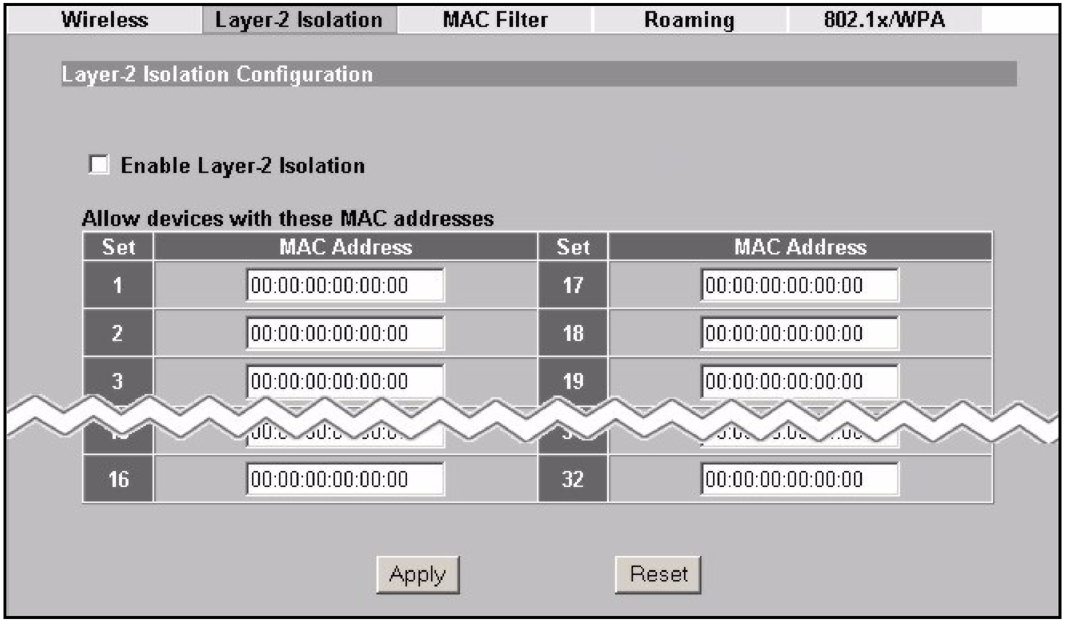
MAC addresses that are not listed in the Allow devices with these MAC addresses table are blocked from communicating with the ZyAIR's wireless clients except for broadcast packets. Layer-2 isolation does not check the traffic between wireless clients that are associated with the same AP. Intra-BSS Traffic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

6.6 Layer-2 Isolation Configuration

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 29 Layer-2 Isolation Configuration Screen



Layer-2 Isolation Configuration

☐ 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
3	00:00:00:00:00:00	19	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this screen.

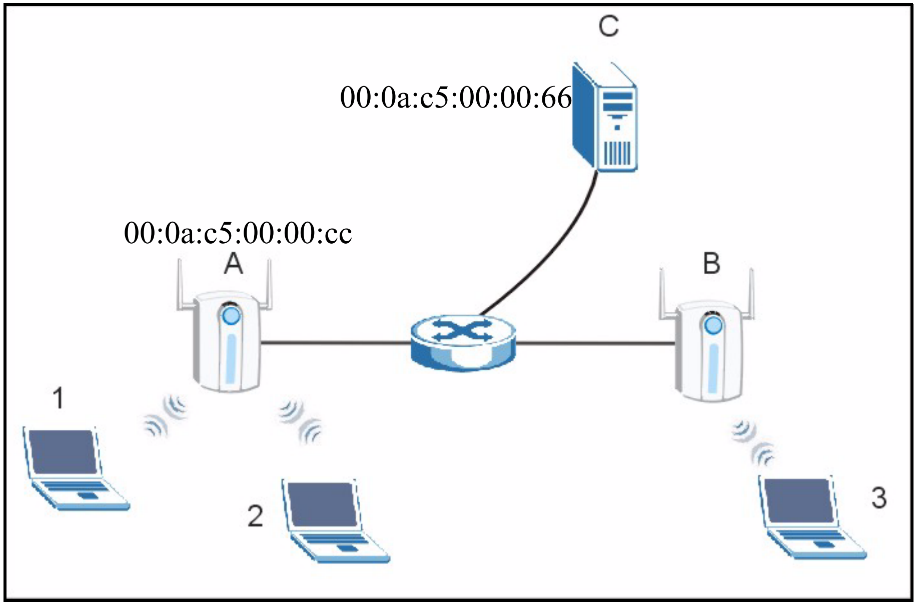
Table 14 Layer-2 Isolation Configuration

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.

6.6.1 Layer-2 Isolation Examples

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

Figure 30 Layer-2 Isolation Example

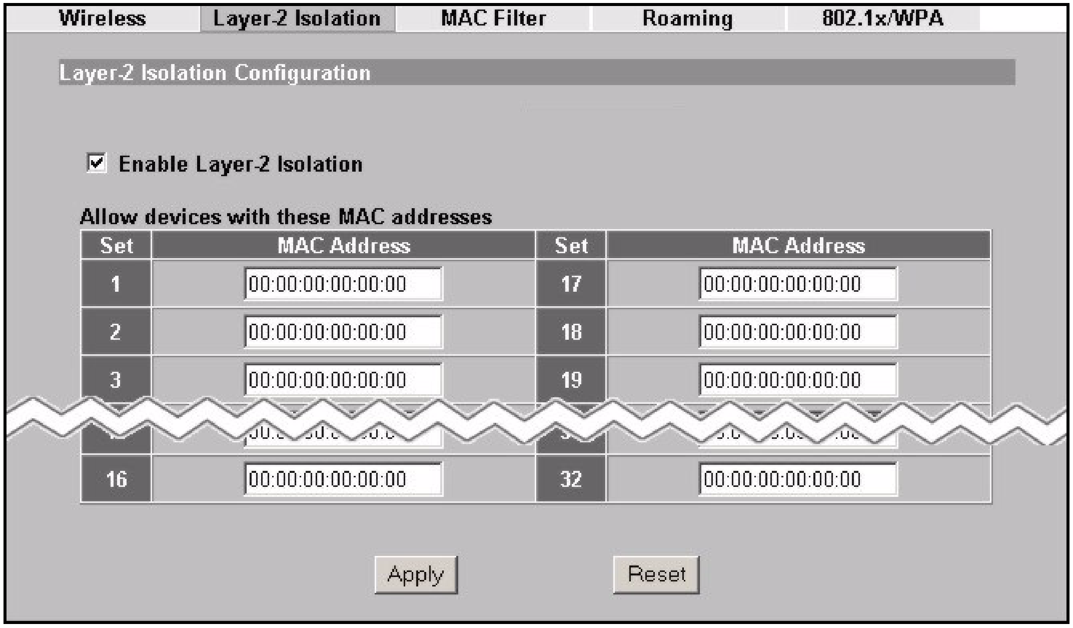


6.6.2 Layer-2 Isolation Example 1

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 31 Layer-2 Isolation Example 1



Layer-2 Isolation Configuration

☑ Enable Layer-2 Isolation

Allow devices with these MAC addresses

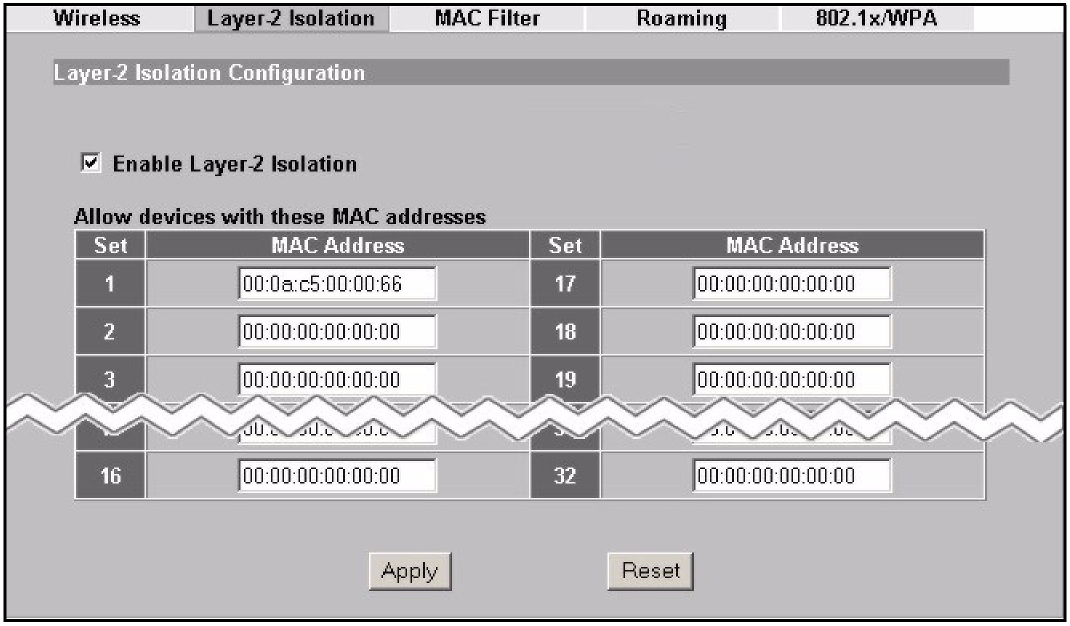
Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

6.6.3 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 32 Layer-2 Isolation Example 2



Layer-2 Isolation Configuration

☑ Enable Layer-2 Isolation

Allow devices with these MAC addresses

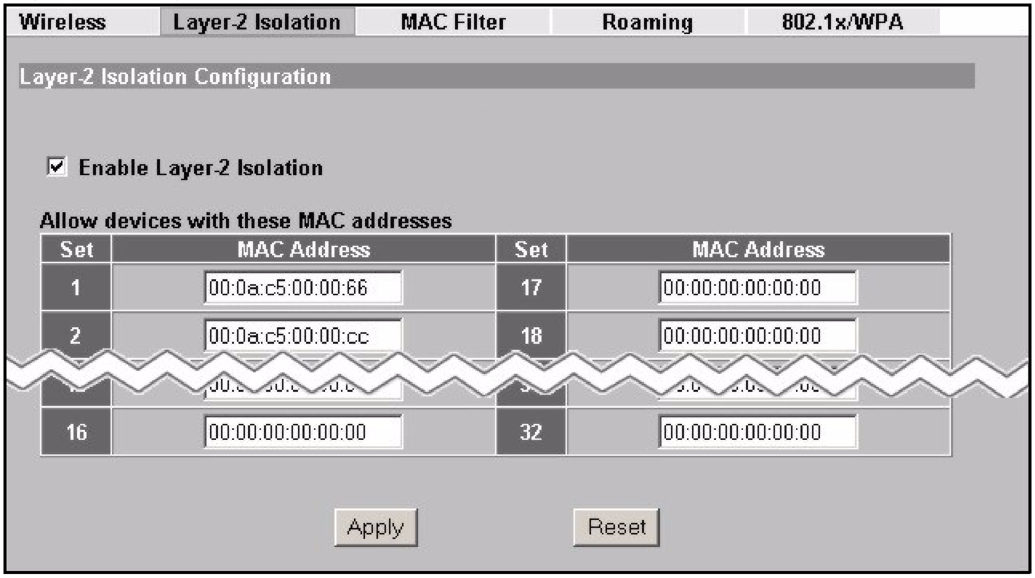
Set	MAC Address	Set	MAC Address
1	00:0a:c5:00:00:66	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

6.6.4 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 33 Layer-2 Isolation Example 3



Layer-2 Isolation Configuration

☑ Enable Layer-2 Isolation

Allow devices with these MAC addresses

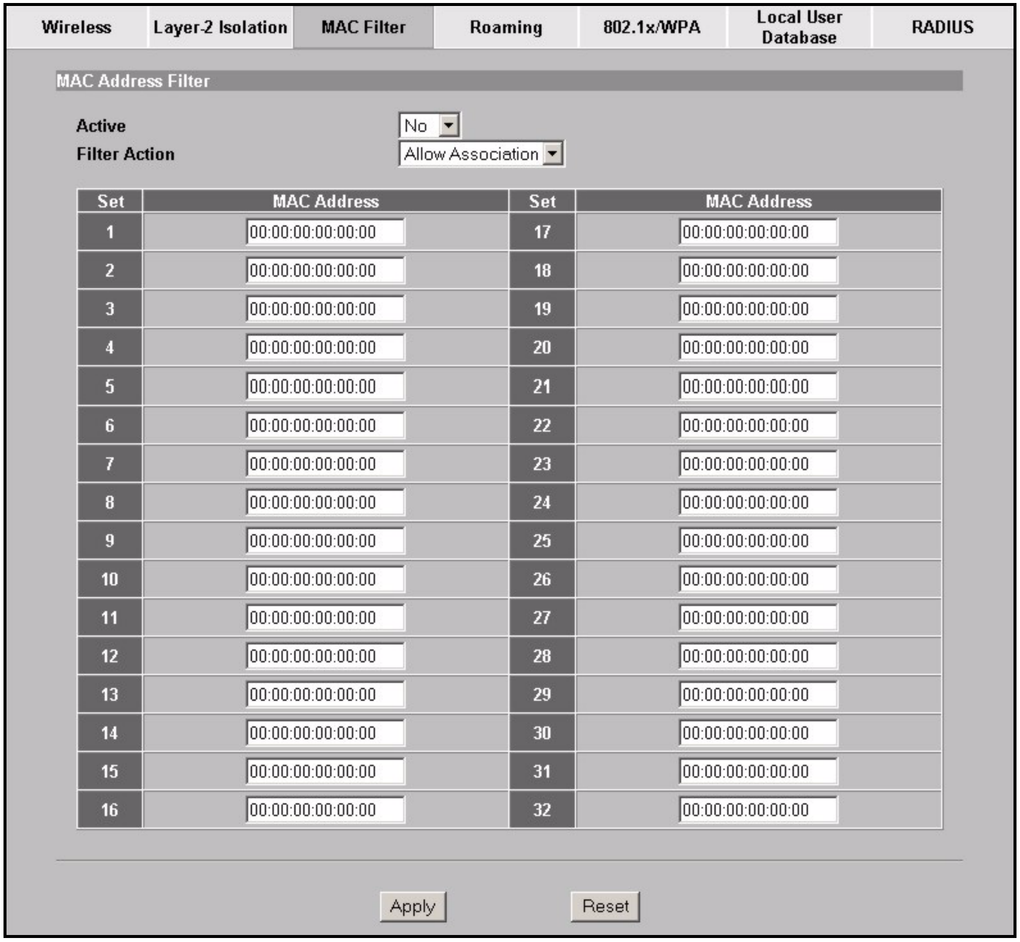
Set	MAC Address	Set	MAC Address
1	00:0a:c5:00:00:66	17	00:00:00:00:00:00
2	00:0a:c5:00:00:cc	18	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

6.7 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 then the **MAC Filter** tab. The screen appears as shown.

Figure 34 MAC Address Filter



MAC Address Filter

Active: No

Filter Action: Allow Association

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

The following table describes the labels in this screen.

Table 15 MAC Address Filter

LABEL	DESCRIPTION
Active	Select Yes from the drop down list box to enable MAC address filtering.
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.

6.8 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA is preferred to WEP as WPA has user authentication and improved data encryption. See the appendix for more information on WPA user authentication and WPA encryption.

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

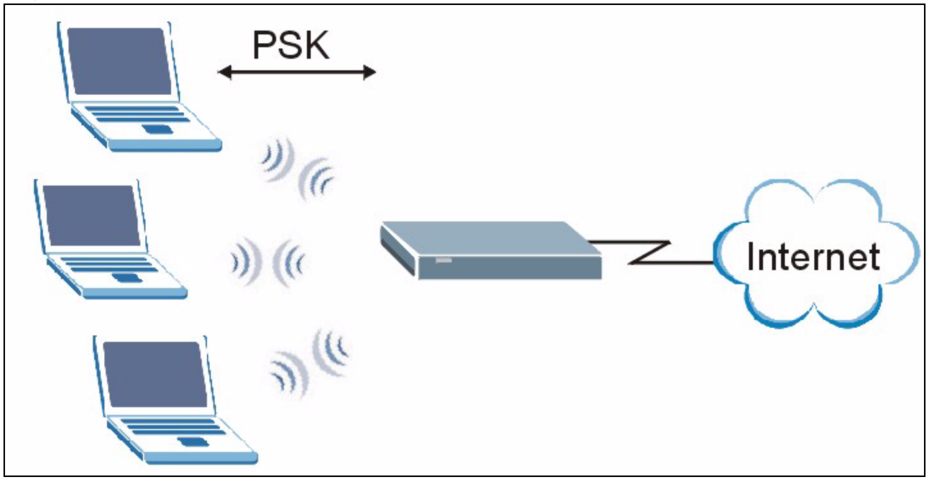
Note: You can't use the Local User Database for authentication when you select WPA.

6.8.1 WPA-PSK Application Example

A WPA-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must be between 8 and 63 printable characters (including spaces; alphabetic characters are case-sensitive).
2. The AP checks each client's password and (only) allows it to join the network if the passwords match.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

Figure 35 WPA - PSK Authentication



6.8.2 WPA with RADIUS Application Example

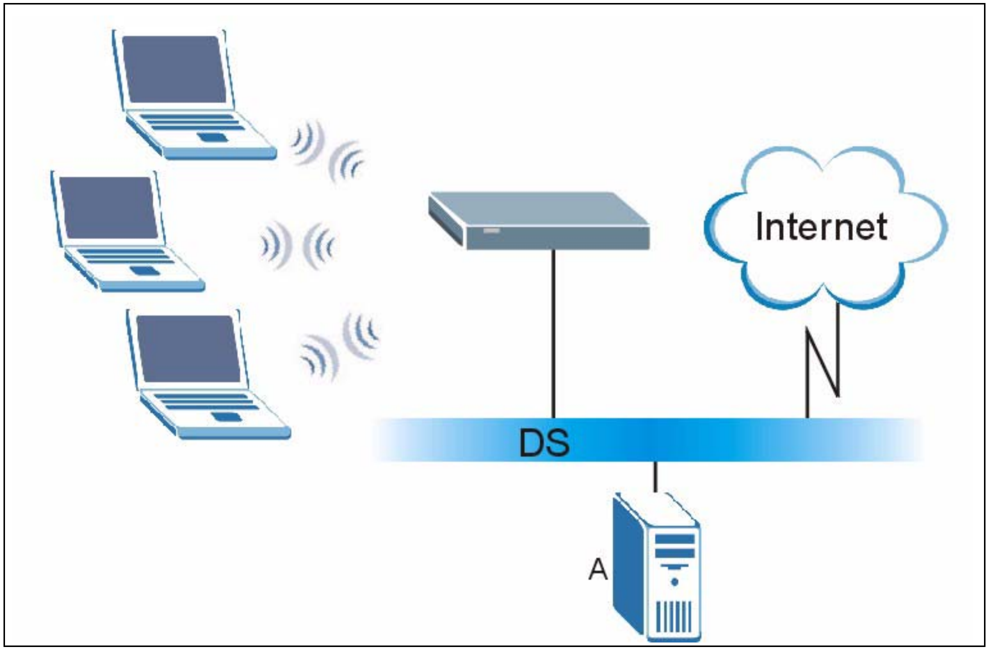
You need the IP address, port number (default is 1812) and shared secret of a RADIUS server. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system (wired link to the LAN).

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 transmitted between the AP and the wireless clients

Figure 36 WPA with RADIUS Application Example2



6.8.3 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 supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

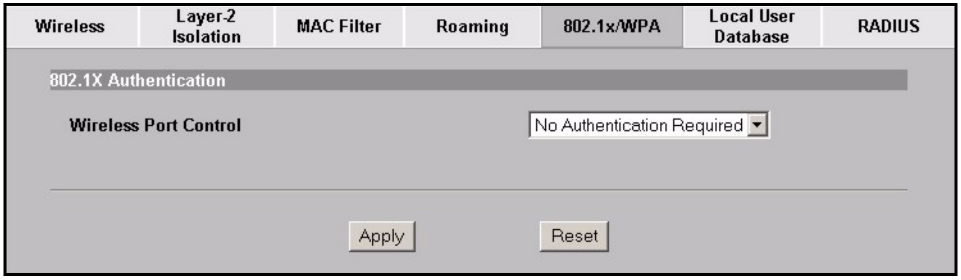
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

6.9 Configuring IEEE 802.1x and WPA

To change your ZyAIR's authentication settings, click the **WIRELESS** link under **ADVANCED** and then the **802.1x/WPA** tab. The screen varies by the key management protocol you select.

You see the next screen when you select **No Access Allowed** or **No Authentication Required** in the **Wireless Port Control field**.

Figure 37 Wireless LAN : 802.1x/WPA



802.1X Authentication

Wireless Port Control: No Authentication Required

The following table describes the labels in this screen.

Table 16 Wireless LAN : 802.1x/WPA

LABEL	DESCRIPTION
Wireless Port Control	To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Access Allowed**, **No Authentication Required** and **Authentication Required**. **No Access Allowed** blocks all wireless stations access to the wired network. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **Authentication Required** to configure **Key Management Protocol** and other related fields.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

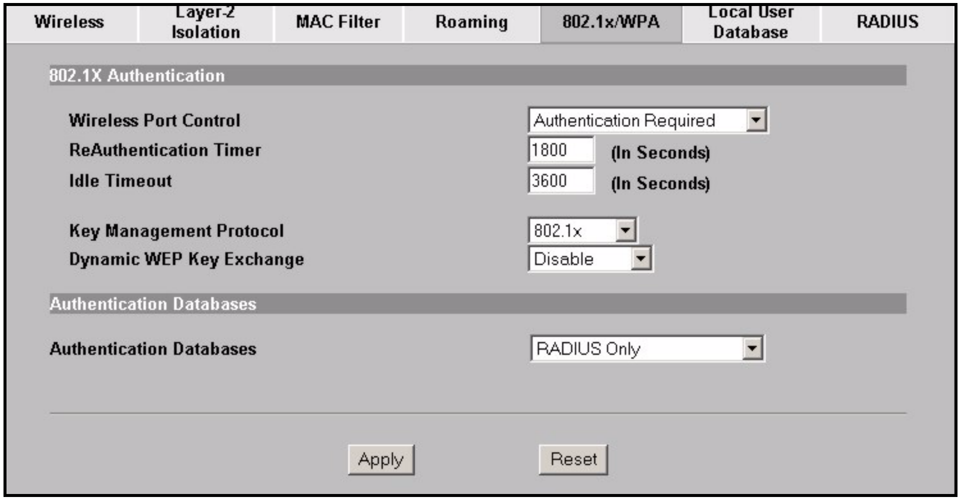
6.9.1 Authentication Required: 802.1x

You need the following for IEEE 802.1x authentication.

- A computer with an IEEE 802.11 a/b/g wireless LAN adapter and equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station computer must be running IEEE 802.1x-compliant software. Not all Windows operating systems support IEEE 802.1x (see the Microsoft web site for details). For other operating systems, see their documentation. If your operating system does not support IEEE 802.1x, then you may need to install IEEE 802.1x client software.
- An optional network RADIUS server for remote user authentication and accounting.

Select **Authentication Required** in the **Wireless Port Control** field and **802.1x** in the **Key Management Protocol** field to display the next screen.

Figure 38 Wireless LAN : 802.1x/WPA for 802.1x Protocol



802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: 802.1x

Dynamic WEP Key Exchange: Disable

Authentication Databases

Authentication Databases: RADIUS Only

The following table describes the labels in this screen.

Table 17 Wireless LAN : 802.1x/WPA for 802.1x Protocol

LABEL	DESCRIPTION
Wireless Port Control	To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Authentication Required**, **Authentication Required** and **No Access Allowed**. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. **No Access Allowed** blocks all wireless stations access to the wired network. The following fields are only available when you select **Authentication Required**.
ReAuthentication Timer (In Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. 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 (In Seconds)	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. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).
Key Management Protocol	Choose **802.1x** from the drop-down list.

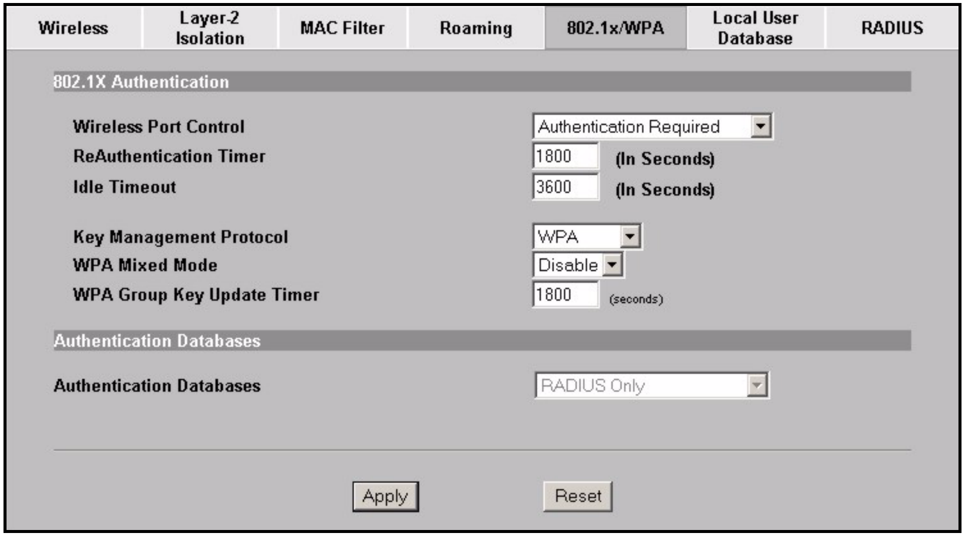
Table 17 Wireless LAN : 802.1x/WPA for 802.1x Protocol

LABEL	DESCRIPTION
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Key Management Protocol** field to **802.1x**. Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the ZyAIR when you configure dynamic WEP key exchange. This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**.
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIRZyAIR. 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. Before you specify the priority, make sure you have set up the corresponding database correctly first. 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. 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. 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. 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.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

6.9.2 Authentication Required : WPA

Select **Authentication Required** in the **Wireless Port Control** field and **WPA** in the **Key Management Protocol** field to display the next screen.

Figure 39 Wireless LAN: 802.1x/WPA for WPA Protocol



802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA

WPA Mixed Mode: Disable

WPA Group Key Update Timer: 1800 (seconds)

Authentication Databases

Authentication Databases: RADIUS Only

The following table describes the labels not previously discussed

Table 18 Wireless LAN: 802.1x/WPA for WPA Protocol

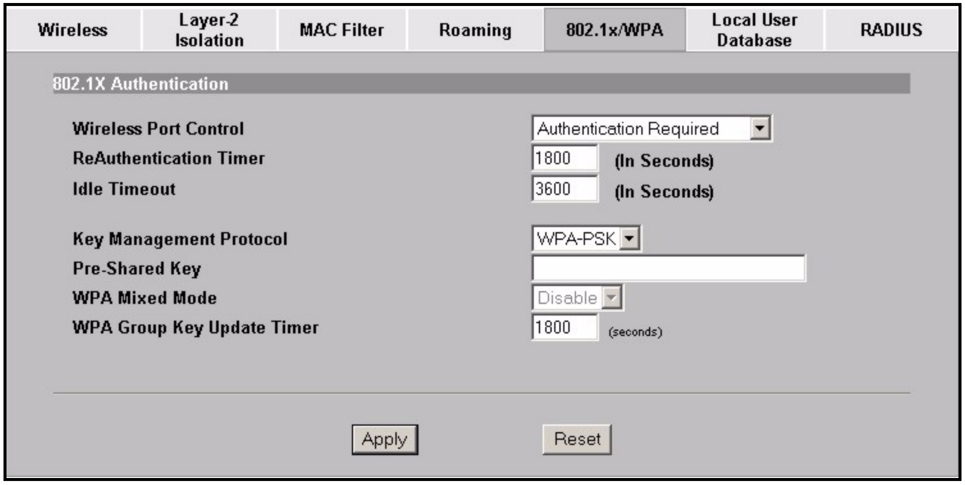
LABEL	DESCRIPTIONS
Key Management Protocol	Choose **WPA** in this field.
WPA Mixed Mode	The ZyAIR can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable**.
WPA Group Key Update Timer	The **WPA 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 **WPA 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.

Refer to table 17 for information on the additional fields shown in this screen.

6.9.3 Authentication Required: WPA-PSK

Select **Authentication Required** in the **Wireless Port Control** field and **WPA-PSK** in the **Key Management Protocol** field to display the next screen.

Figure 40 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol



Wireless Port Control: Authentication Required
ReAuthentication Timer: 1800 (In Seconds)
Idle Timeout: 3600 (In Seconds)
Key Management Protocol: WPA-PSK
Pre-Shared Key:
WPA Mixed Mode: Disable
WPA Group Key Update Timer: 1800 (seconds)

The following table describes the labels not previously discussed

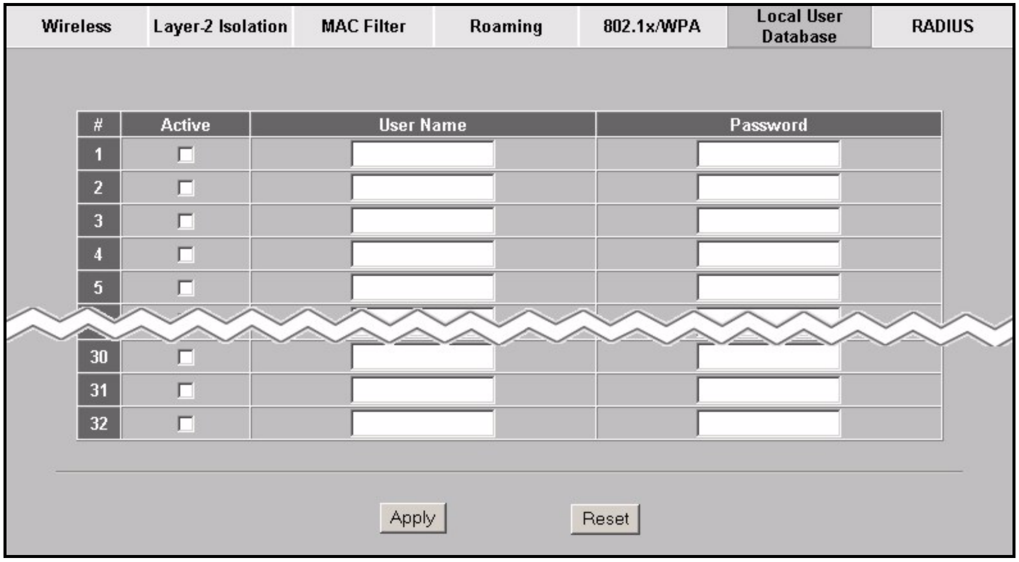
Table 19 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

LABEL	DESCRIPTION
Key Management Protocol	Choose **WPA-PSK** 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).
WPA Mixed Mode	This field is disabled for WPA-PSK key management protocol.
WPA Group Key Update Timer	The **WPA 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 **WPA 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.

6.10 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 41 Local User Database



The following table describes the labels in this screen.

Table 20 Local User Database

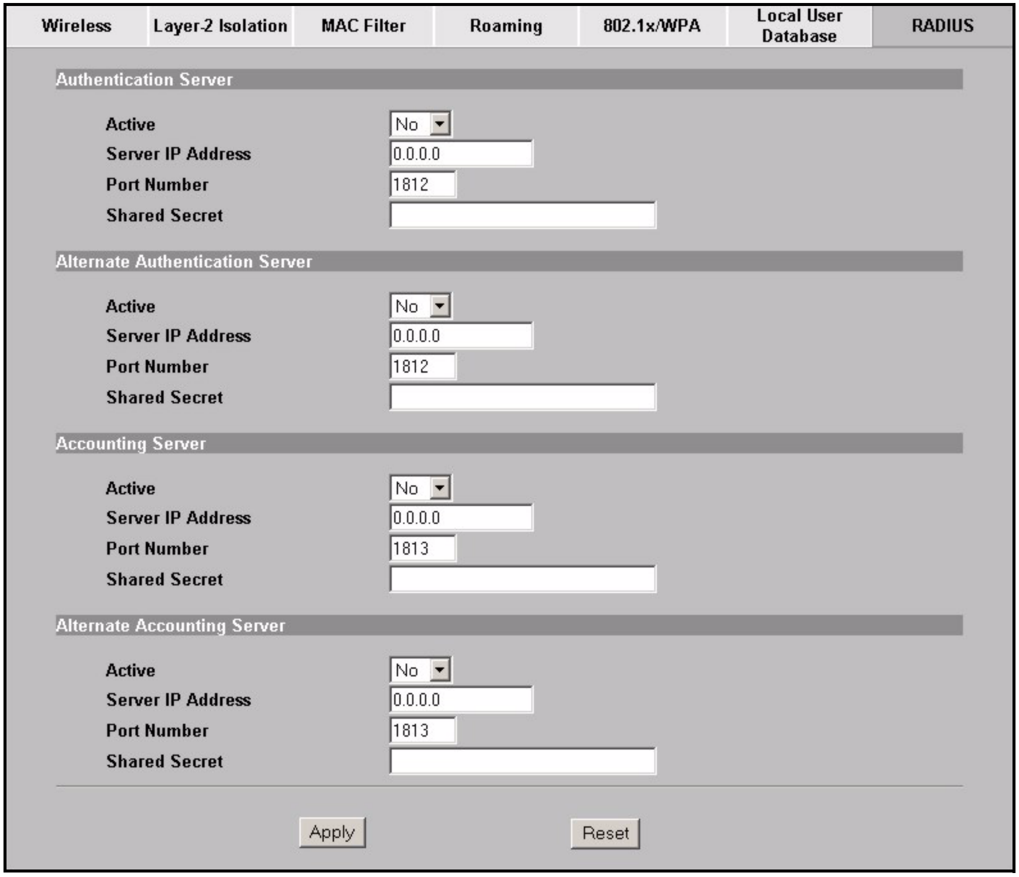
LABEL	DESCRIPTION
Active	Select this check box to activate the user profile.
User Name	Enter the username (up to 31 characters) for this user profile.
Password	Type a password (up to 31 characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you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

6.11 Configuring RADIUS

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

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 42 RADIUS



Authentication Server

Active: No
Server IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Alternate Authentication Server

Active: No
Server IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Accounting Server

Active: No
Server IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:

Alternate Accounting Server

Active: No
Server IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:

The following table describes the labels in this screen.

Table 21 RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select **Yes** from the drop-down list box to enable user authentication through an external authentication server. Select **No** to enable user authentication using the local user database on the ZyAIR.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 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.

Table 21 RADIUS

LABEL	DESCRIPTION
Alternate Authentication Server	If the ZyAIR cannot authenticate wireless users using the **Authentication Server**, the alternative authentication server is used. The ZyAIR will attempt to authenticate three times before using the **Alternate Authentication Server**. Requests can be issued from the client interface to use the alternate authentication 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 **802.1x/WPA** screen. **Note:** You can configure the ZyAIR to use up to five authentication servers in the command line interface.
Active	Select **Yes** from the drop-down list box to enable user authentication through an external authentication server. Select **No** to enable user authentication using the local user database on the ZyAIR.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 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.
Accounting Server	
Active	Select Yes from the drop down list box to enable user accounting through an external authentication server.Select No to enable user accounting using the local user database on the ZyAIR.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	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.
Shared 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.
Alternate Accounting Server	If the ZyAIR cannot communicate with the server, the alternative accounting server is used. The ZyAIR will attempt to communicate three times before using the Alternate Accounting Server. **Note:** You can configure the ZyAIR to use up to five accounting servers in the command line interface.
Active	Select Yes from the drop down list box to enable user accounting through an external authentication server.Select No to enable user accounting using the local user database on the ZyAIR.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	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.

Table 21 RADIUS

LABEL	DESCRIPTION
Shared 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.

CHAPTER 7 Multiple ESS and VLAN

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).

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

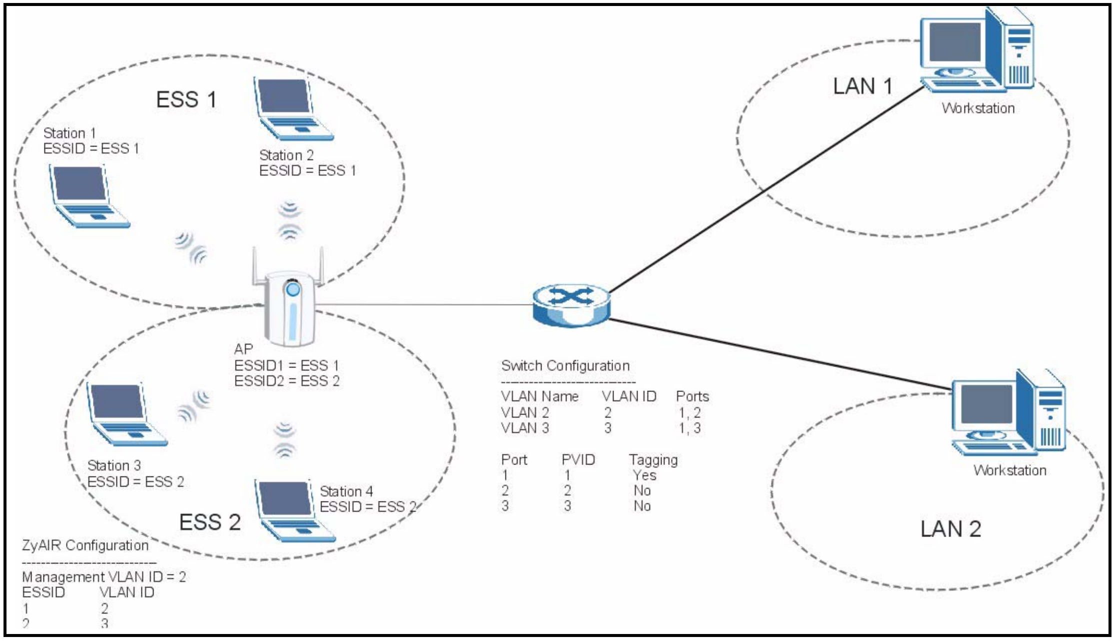
Refer to the section on ZyAIR applications for more information.

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” ESS1is 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 43 Multi-ESS with VLAN Example



Switch Configuration

VLAN Name	VLAN ID	Ports
VLAN 2	2	1, 2
VLAN 3	3	1, 3

Port	PVID	Tagging
1	1	Yes
2	2	No
3	3	No

ZyAIR Configuration

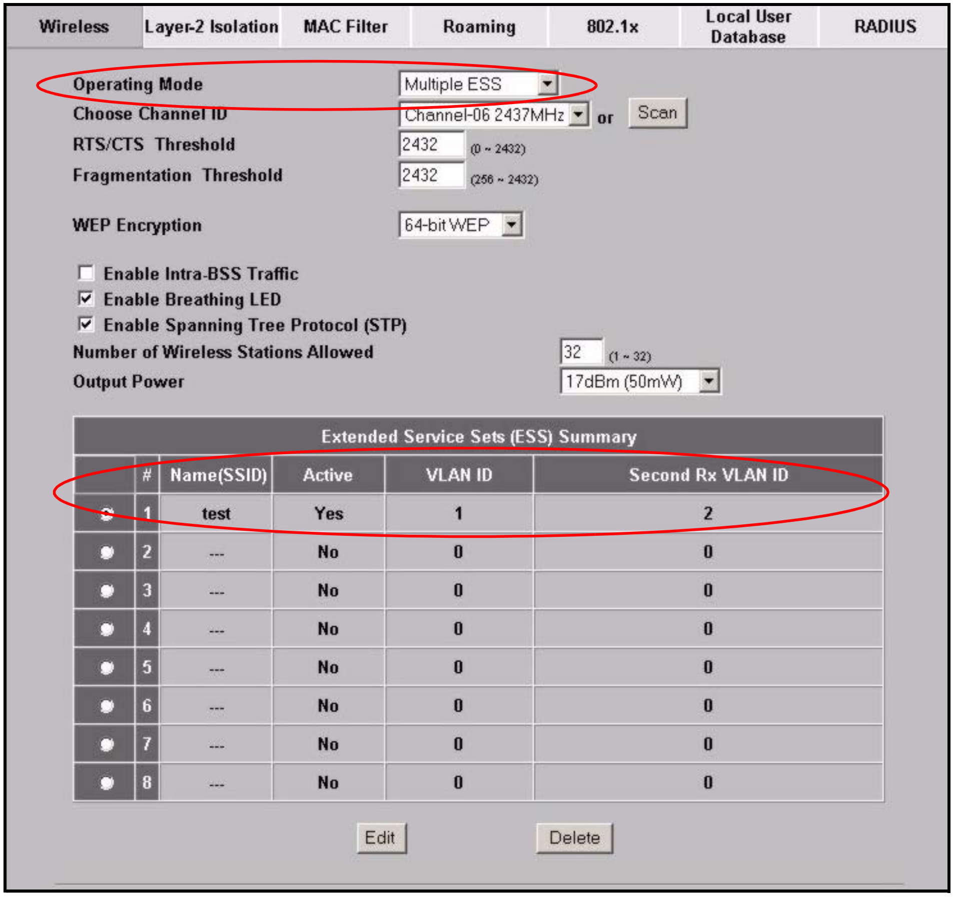
Management VLAN ID = 2

ESSID	VLAN ID
1	2
2	3

7.1.5 Configuring Multiple ESS

Click the **WIRELESS** link under **ADVANCED**. Select **Multiple ESS** in the **Operating Mode** drop-down list box to display the screen as shown.

Figure 44 Wireless : Multiple ESS



Operating Mode: Multiple ESS
Choose Channel ID: Channel-06 2437MHz or Scan
RTS/CTS Threshold: 2432 (0 ~ 2432)
Fragmentation Threshold: 2432 (256 ~ 2432)
WEP Encryption: 64-bit WEP

☐ Enable Intra-BSS Traffic
☑ Enable Breathing LED
☑ Enable Spanning Tree Protocol (STP)

Number of Wireless Stations Allowed: 32 (1 ~ 32)
Output Power: 17dBm (50mW)

Extended Service Sets (ESS) Summary

	#	Name(SSID)	Active	VLAN ID	Second Rx VLAN ID
●	1	test	Yes	1	2
○	2	---	No	0	0
○	3	---	No	0	0
○	4	---	No	0	0
○	5	---	No	0	0
○	6	---	No	0	0
○	7	---	No	0	0
○	8	---	No	0	0

The following table describes the labels in this screen.

Table 22 Wireless: Multiple ESS

LABEL	DESCRIPTION
Operating Mode	Select Multiple ESS 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.
Extended Service Set (ESS) Summary	
#	This is the index number of each ESS.
Name(SSID)	This is the identification name of each ESS.
Active	This field displays **Yes** if the ESS is active and **No** if it is not.
VLAN ID	This is the identification number of each VLAN.

Table 22 Wireless: Multiple ESS

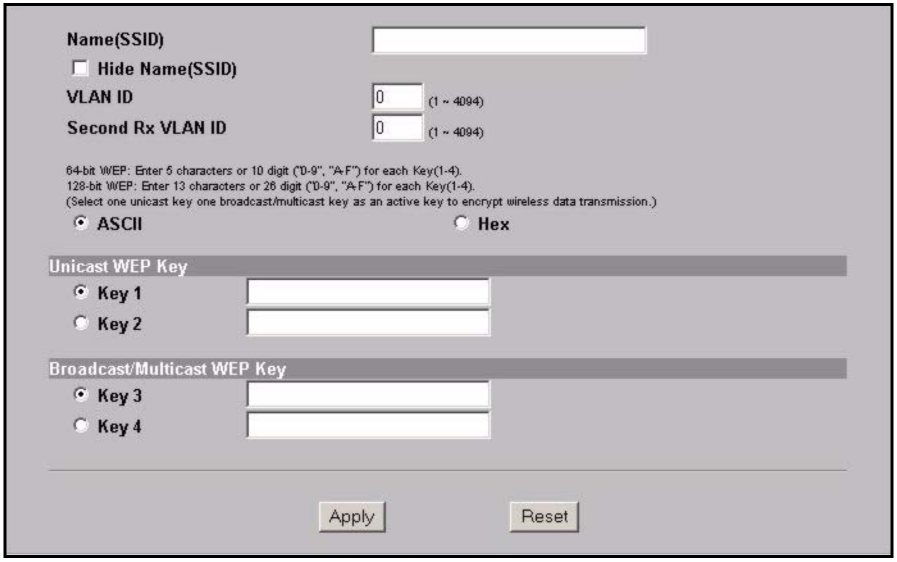
LABEL	DESCRIPTION
Second Rx VLAN ID	This field displays the identification number of incoming Ethernet frames that are forwarded to this ESS. This number can be the same for many ESS groups, depending on how many you want to be members of a particular VLAN.
Edit	Select the radio button next to the ESS index you want to configure and click Edit to go to the **EDIT ESS** screen.
Delete	Select the radio button next to the ESS index you want to remove and click **Delete** to remove the ESS.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

7.1.5.1 Edit ESS

Note: You must configure at least one ESS ID to activate multiple ESS on the ZyAIR

Click **Edit** in the **Wireless** screen.

Figure 45 Wireless : Edit ESS



Name(SSID)	
□ Hide Name(SSID)	
VLAN ID	0 (1 ~ 4094)
Second Rx VLAN ID	0 (1 ~ 4094)

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one unicast key one broadcast/multicast key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

Unicast WEP Key

● Key 1
○ Key 2

Broadcast/Multicast WEP Key

● Key 3
○ Key 4

The following table describes the labels in this screen.

Table 23 Wireless: Edit ESS

LABEL	DESCRIPTION
Name(SSID)	Enter a descriptive name (up to 32 alphanumeric characters) for identification purposes. This name is case sensitive.
Active	Select this check box to activate this ESS.
VLAN ID	Enter a number from 1 to 4094.
Second Rx VLAN ID	Enter a number from 1 to 4094, but different to the VLAN ID entered.
ASCII	Select this option to enter ASCII characters as the WEP keys.

Table 23 Wireless: Edit ESS

LABEL	DESCRIPTION
Hex	Select this option to enter hexadecimal characters as the WEP keys.The preceding "0x" is entered automatically.
Unicast WEP key	
Key 1 or Key 2	Key 1 or key 2 is used to encrypt unicast transmissions. 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 both keys, but only one key can be activated at any one time. The default key is key 1.
Broadcast/Multicast WEP key	
Key 3 or Key 4	Key 3 or key 4 is used to encrypt multicast/broadcast transmissions. 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 both keys, but only one key can be activated at any one time. The default key is key 3.
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

7.2 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.

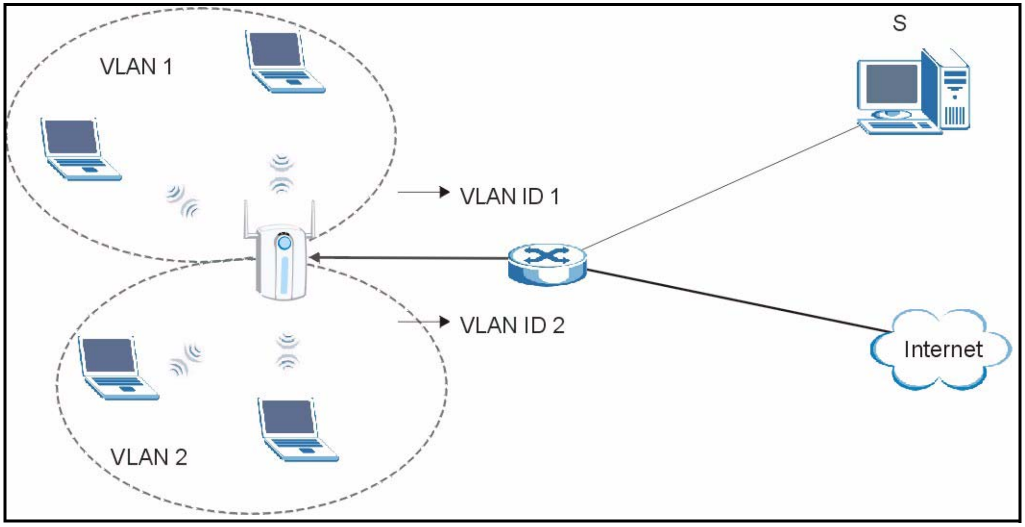
7.2.1 VLAN Tagging

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.

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. See the table in Figure 7?2.

Figure 46 Second Rx VLAN ID Example



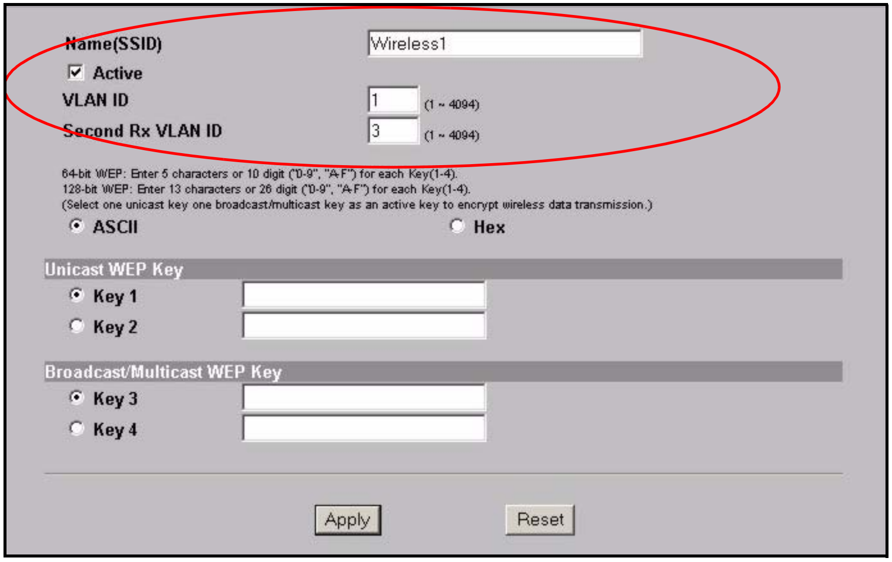
The following steps show you where to setup a Second Rx VLAN ID on the ZyAIR.

1 Click **WIRELESS** under **ADVANCED** in your web configurator.

2 Click **Edit** in the wireless screen. The operating mode should be set as **Multiple ESS**.

3 You can enter a **Second Rx VLAN ID** in the following screen.

Figure 47 Edit ESS : Second Rx VLAN ID Example



Name(SSID): Wireless1

☑ Active

VLAN ID: 1 (1 ~ 4094)

Second Rx VLAN ID: 3 (1 ~ 4094)

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one unicast key one broadcast/multicast key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

Unicast WEP Key

● Key 1
○ Key 2

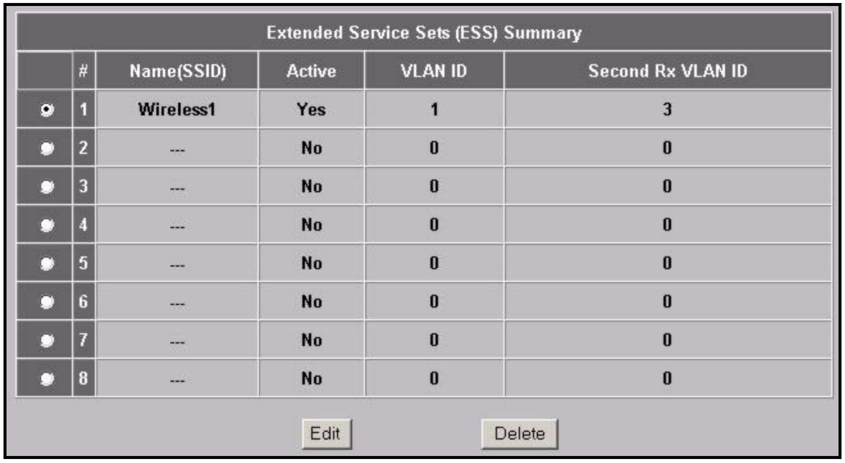
Broadcast/Multicast WEP Key

● Key 3
○ Key 4

4 Click **Apply** to save these settings to the ZyAIR and to return to the **Wireless** screen.

5 An ESS summary screen is displayed in the **Wireless** screen. This 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 48   ESS – VLAN ID and Second Rx VLAN ID Example



Extended Service Sets (ESS) Summary

	#	Name(SSID)	Active	VLAN ID	Second Rx VLAN ID
◉	1	Wireless1	Yes	1	3
○	2	---	No	0	0
○	3	---	No	0	0
○	4	---	No	0	0
○	5	---	No	0	0
○	6	---	No	0	0
○	7	---	No	0	0
○	8	---	No	0	0

7.2.3 Management VLAN ID

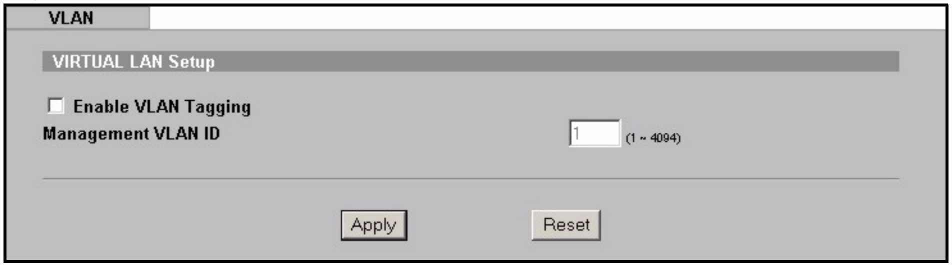
The management VLAN ID identifies the “management VLAN”. A device must be a member of this “management VLAN” in order to access and manage the ZyAIR. If a device is not a member of this VLAN, then that device cannot manage the ZyAIR.

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.

7.2.4 Configuring VLAN

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

Figure 49   VLAN



□ Enable VLAN Tagging

Management VLAN ID 1 (1 ~ 4094)

The following table describes the labels in this screen.

Table 24   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 group in order to manage the ZyAIR. **Note:** Mail and FTP servers must have the same management VLAN ID to communicate with the ZyAIR.

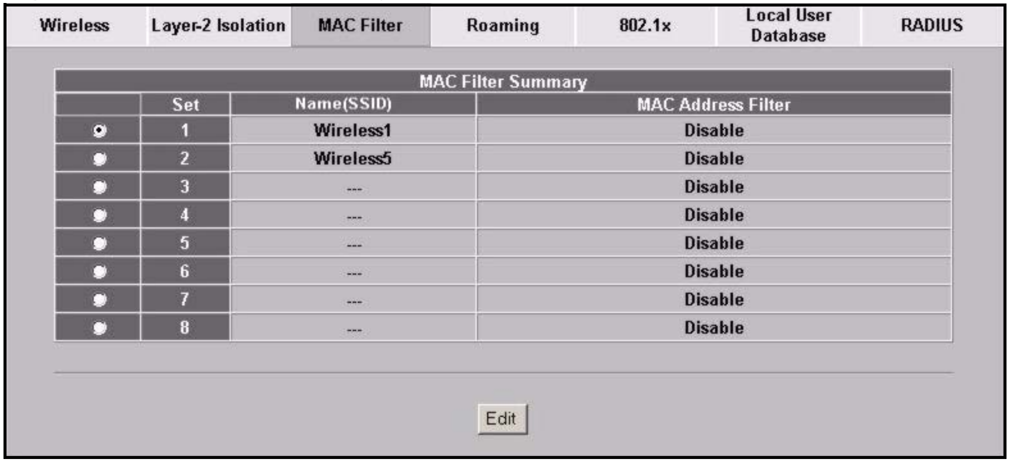
Table 24 VLAN

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyAIR.
Reset	Click **Reset** to begin configuring this screen afresh.

7.3 MAC Filter Summary

If you select **Multiple ESS** in the **Operating Mode** field in the **Wireless** screen, the **MAC Filter Summary** screen displays as shown when you click the **MAC Filter** tab.

Figure 50 MAC Filter Summary



MAC Filter Summary

	Set	Name(SSID)	MAC Address Filter
●	1	Wireless1	Disable
○	2	Wireless5	Disable
○	3	---	Disable
○	4	---	Disable
○	5	---	Disable
○	6	---	Disable
○	7	---	Disable
○	8	---	Disable

The following table describes the labels in this screen.

Table 25 MAC Filter Summary

LABEL	DESCRIPTION
Set	This is the index number of each ESS.
Name(SSID)	This is the identification name of each ESS.
MAC Address Filter	This field displays **Disable** if the MAC filter is inactive, **Association Allowed** if the MAC filter is active and filter action is allowed or **Association Denied** if the MAC filter is active but filter action is denied.
Edit	Click the radio button next to the set you want to configure and click Edit to go to the **MAC Address Filter** screen. Refer to the **MAC Filter** section.

CHAPTER 8
IP Screen

This chapter discusses how to configure IP on the ZyAIR

8.1 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.

8.2 TCP/IP Parameters

8.2.1 IP Address and Subnet Mask

Refer to the IP Address and Subnet Mask section in the Wizard Setup chapter for this information.

8.2.2 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 26 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

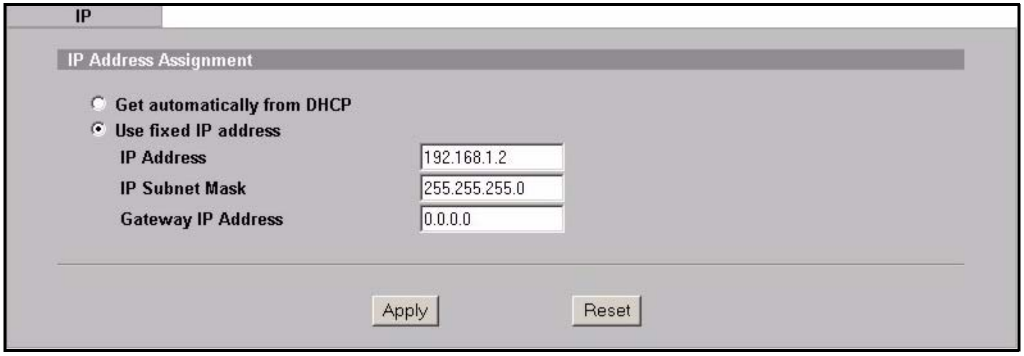
You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much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

8.3 Configuring IP

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

Figure 51 IP Setup



IP

IP Address Assignment

○ Get automatically from DHCP

● Use fixed IP address

IP Address: 192.168.1.2

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

Table 27 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 9
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.

9.1 Configuring View Log

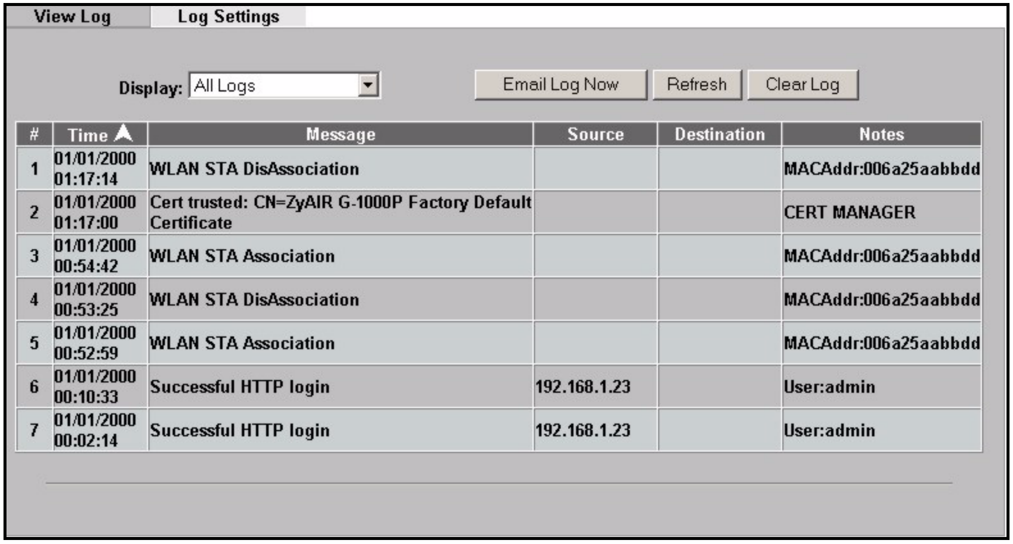
The web configurator allows you to look at all of the ZyAIR's logs in one location.

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 53). 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 52 View Log



Display: All Logs

#	Time	Message	Source	Destination	Notes
1	01/01/2000 01:17:14	WLAN STA DisAssociation			MACAddr:006a25aabbdd
2	01/01/2000 01:17:00	Cert trusted: CN=ZyAIR G-1000P Factory Default Certificate			CERT MANAGER
3	01/01/2000 00:54:42	WLAN STA Association			MACAddr:006a25aabbdd
4	01/01/2000 00:53:25	WLAN STA DisAssociation			MACAddr:006a25aabbdd
5	01/01/2000 00:52:59	WLAN STA Association			MACAddr:006a25aabbdd
6	01/01/2000 00:10:33	Successful HTTP login	192.168.1.23		User:admin
7	01/01/2000 00:02:14	Successful HTTP login	192.168.1.23		User:admin

The following table describes the labels in this screen.

Table 28 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.
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.

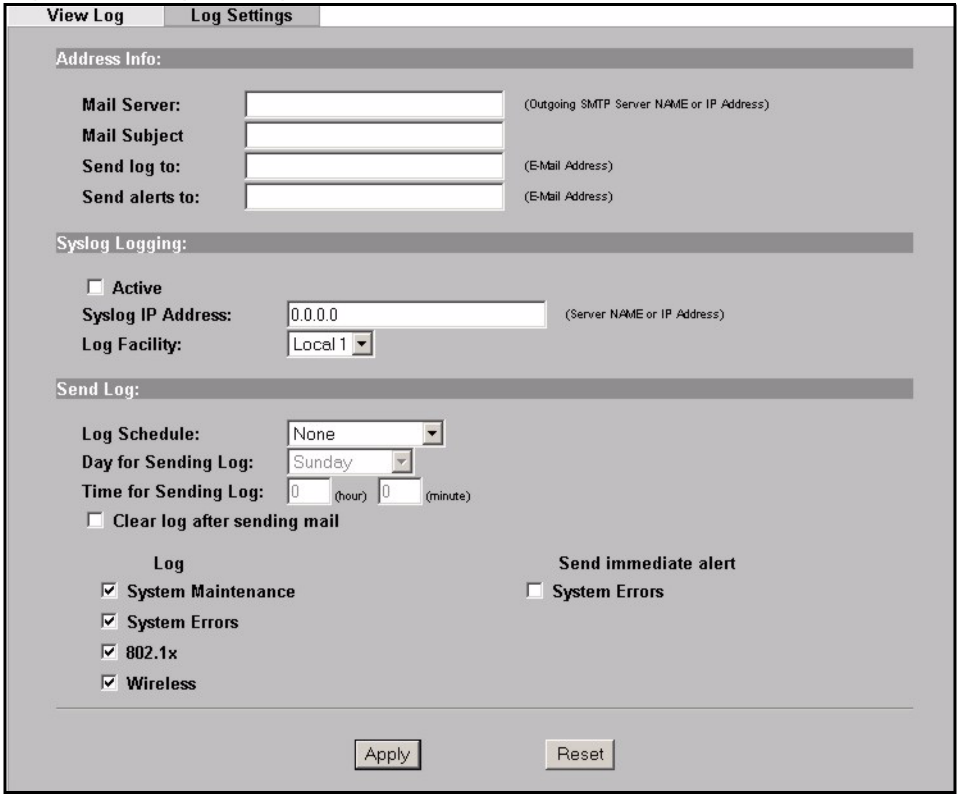
9.2 Configuring Log Settings

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 53   Log Settings



Address Info:

Mail Server: (Outgoing SMTP Server NAME or IP Address)

Mail Subject

Send log to: (E-Mail Address)

Send alerts to: (E-Mail Address)

Syslog Logging:

□ Active

Syslog IP Address: 0.0.0.0 (Server NAME or IP Address)

Log Facility: Local 1

Send Log:

Log Schedule: None

Day for Sending Log: Sunday

Time for Sending Log: 0 (hour) 0 (minute)

□ Clear log after sending mail

Log

☑ System Maintenance

☑ System Errors

☑ 802.1x

☑ Wireless

Send immediate alert

□ System Errors

The following table describes the labels in this screen.

Table 29   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.

Table 29 Log Settings

LABEL	DESCRIPTION
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	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. 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.
Day for Sending Log	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.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select the categories of alerts for which you want the ZyAIR to immediately send e-mail alerts.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to reconfigure all the fields in this screen.

CHAPTER 10 Maintenance

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

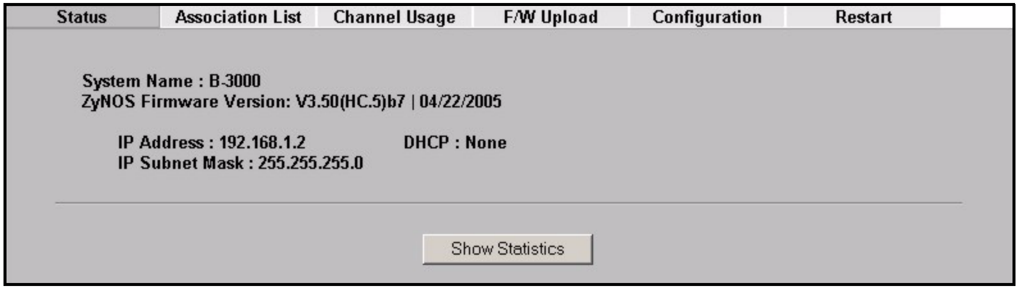
10.1 Maintenance Overview

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

10.2 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 54 System Status



System Name : B-3000
ZyNOS Firmware Version: V3.50(HC.5)b7 | 04/22/2005

IP Address : 192.168.1.2
IP Subnet Mask : 255.255.255.0
DHCP : None

The following table describes the labels in this screen.

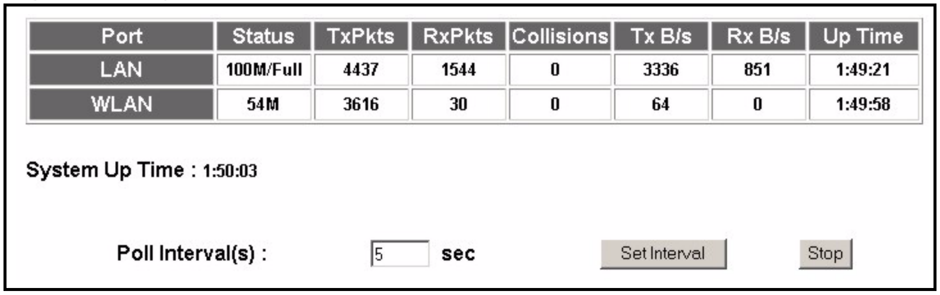
Table 30 System Status

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.

10.2.1 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 55   System Status: Show Statistics



Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	4437	1544	0	3336	851	1:49:21
WLAN	54M	3616	30	0	64	0	1:49:58

System Up Time : 1:50:03

Poll Interval(s) : 5 sec

The following table describes the labels in this screen.

Table 31   System Status: Show Statistics

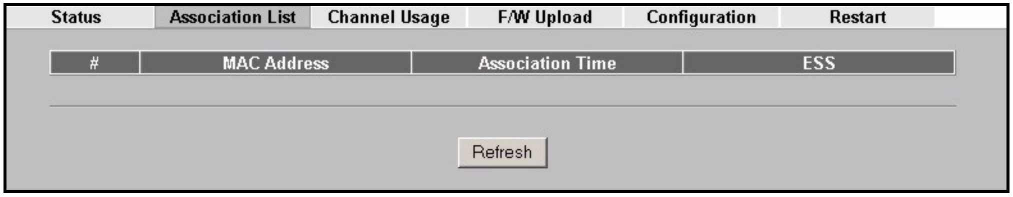
LABEL	DESCRIPTION
Port	This is the Ethernet or wireless port. The wireless port may be the **WLAN – Built-in** card or the **WLAN – Removable** wireless card.
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. This shows the transmission 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.
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.

10.3 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 56 Association List



The following table describes the labels in this screen.

Table 32 Association List

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

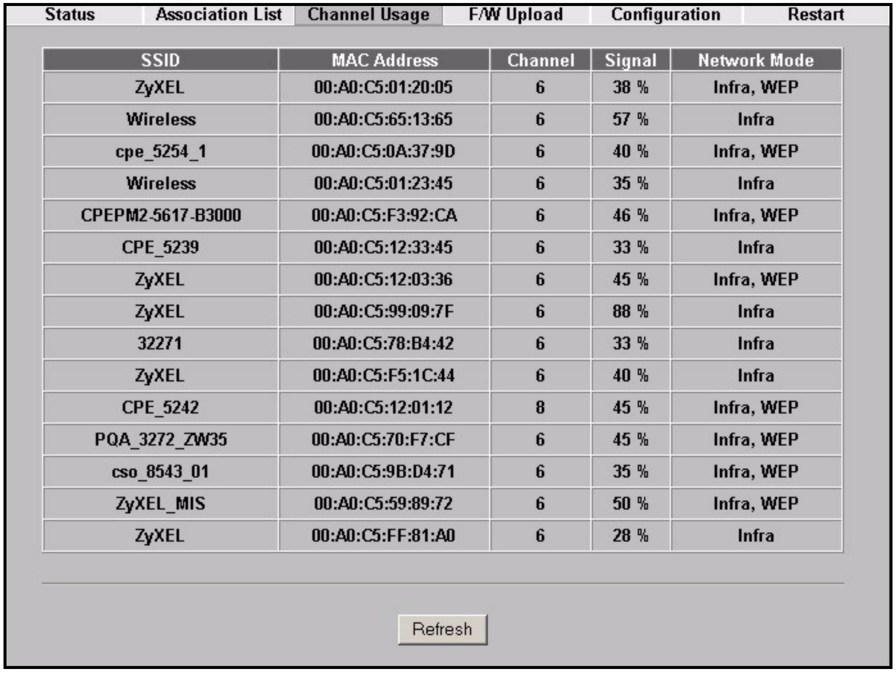
10.4 Channel Usage

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 57 Channel Usage



SSID	MAC Address	Channel	Signal	Network Mode
ZyXEL	00:A0:C5:01:20:05	6	38 %	Infra, WEP
Wireless	00:A0:C5:65:13:65	6	57 %	Infra
cpe_5254_1	00:A0:C5:0A:37:9D	6	40 %	Infra, WEP
Wireless	00:A0:C5:01:23:45	6	35 %	Infra
CPEPM2-5617-B3000	00:A0:C5:F3:92:CA	6	46 %	Infra, WEP
CPE_5239	00:A0:C5:12:33:45	6	33 %	Infra
ZyXEL	00:A0:C5:12:03:36	6	45 %	Infra, WEP
ZyXEL	00:A0:C5:99:09:7F	6	88 %	Infra
32271	00:A0:C5:78:B4:42	6	33 %	Infra
ZyXEL	00:A0:C5:F5:1C:44	6	40 %	Infra
CPE_5242	00:A0:C5:12:01:12	8	45 %	Infra, WEP
PQA_3272_ZW35	00:A0:C5:70:F7:CF	6	45 %	Infra, WEP
cso_8543_01	00:A0:C5:9B:D4:71	6	35 %	Infra, WEP
ZyXEL_MIS	00:A0:C5:59:89:72	6	50 %	Infra, WEP
ZyXEL	00:A0:C5:FF:81:A0	6	28 %	Infra

The following table describes the labels in this screen.

Table 33 Channel Usage

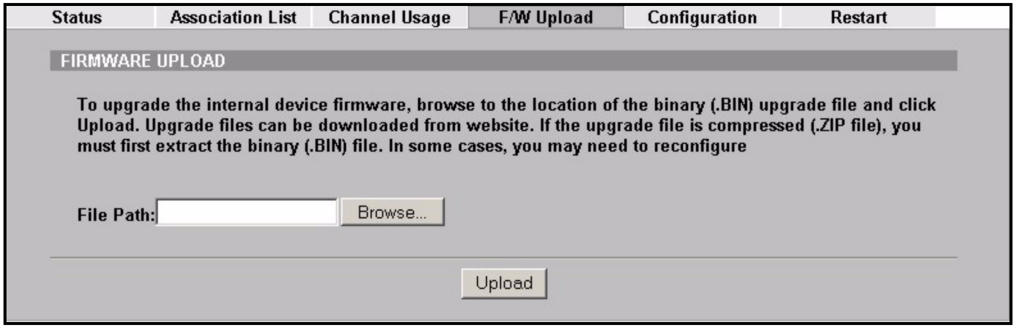
LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the Wireless LAN appendix 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.
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.

10.5 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 58 Firmware Upload



To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure

The following table describes the labels in this screen.

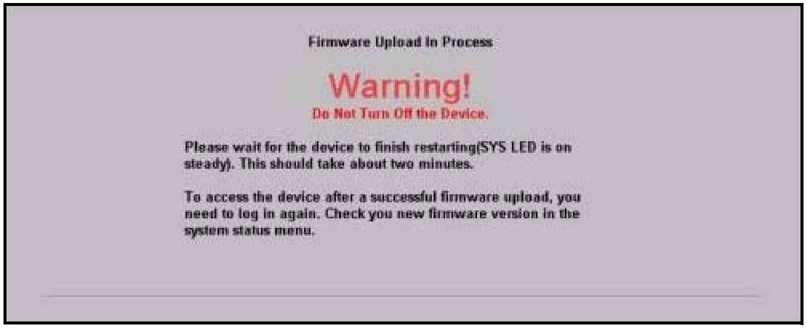
Table 34 Firmware Upload

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 59   Firmware Upload In Process



Firmware Upload In Process

Warning!

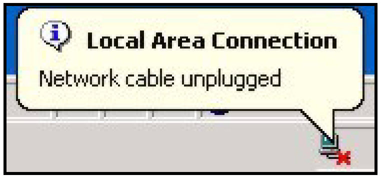
Do Not Turn Off the Device.

Please wait for the device to finish restarting(SYS LED is on steady). This should take about two minutes.

To access the device after a successful firmware upload, you need to log in again. Check you new firmware version in the system status menu.

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 60   Network Temporarily Disconnecte



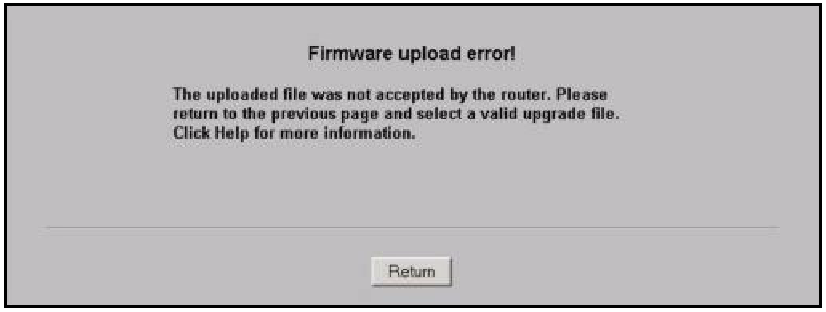
Local Area Connection

Network cable unplugged

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 61   Firmware Upload Error



Firmware upload error!

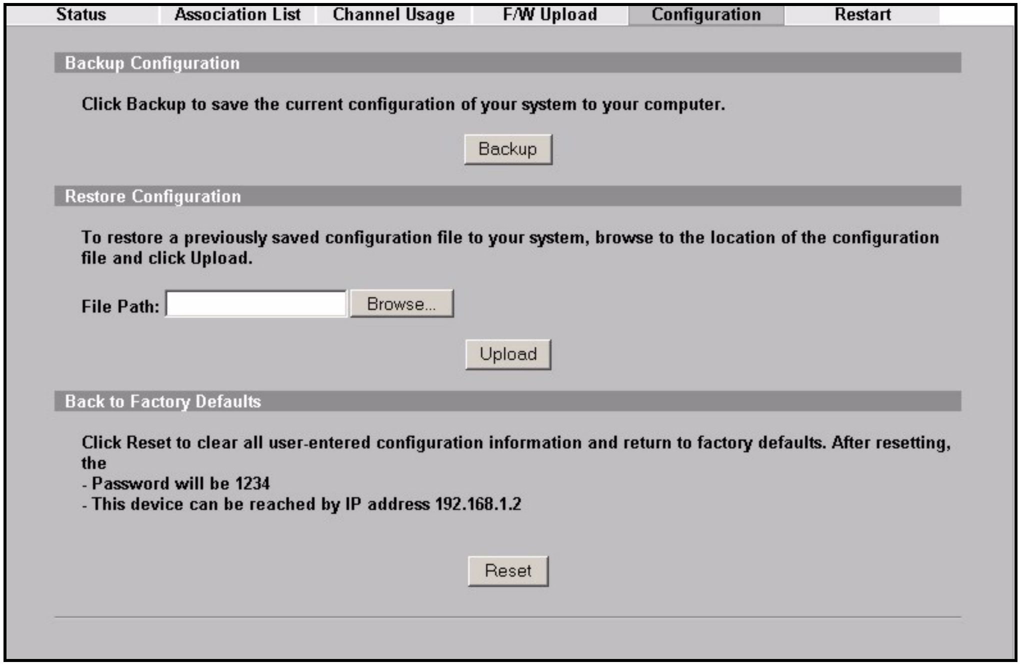
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

10.6 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 62 Configuration



Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path:

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- This device can be reached by IP address 192.168.1.2

10.6.1 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.

10.6.2 Restore Configuration

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

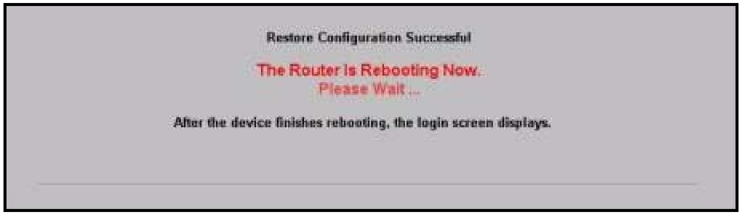
Table 35 Restore Configuration

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 63 Configuration Upload Successful



Restore Configuration Successful

The Router is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

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.

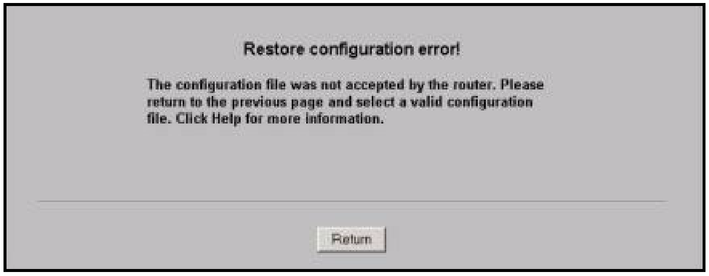
Figure 64 Network Temporarily Disconnected

Local Area Connection
Network cable unplugged

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 65 Configuration Upload Error



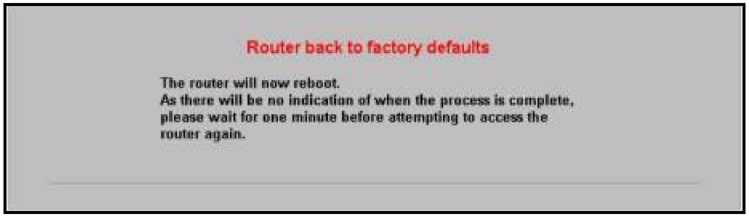
Restore configuration error!

The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.

10.6.3 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 66   Reset Warning Message



Router back to factory defaults

The router will now reboot.
As there will be no indication of when the process is complete,
please wait for one minute before attempting to access the
router again.

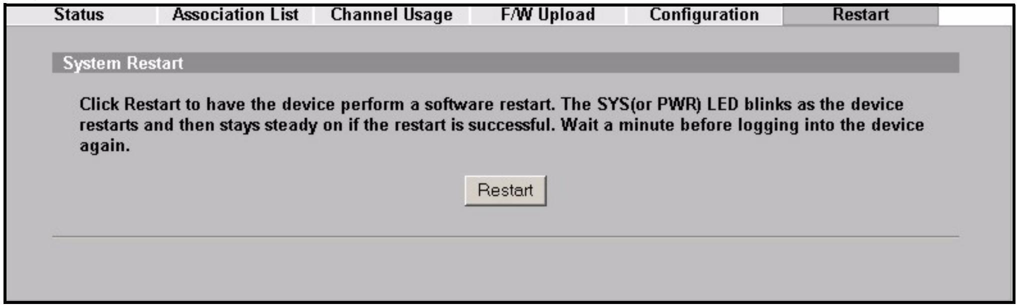
You can also press the **RESET** button on the side panel to reset the factory defaults of your ZyAIR. Refer to the section on resetting the ZyAIR for more information on the **RESET** button.

10.7 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 67   Restart Screen



System Restart

Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.

CHAPTER 11 Introducing the SMT

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

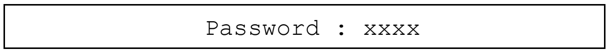
11.1 Connect to your ZyAIR Using Telnet

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 68 Login Screen



```
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.

11.2 Changing the System Password

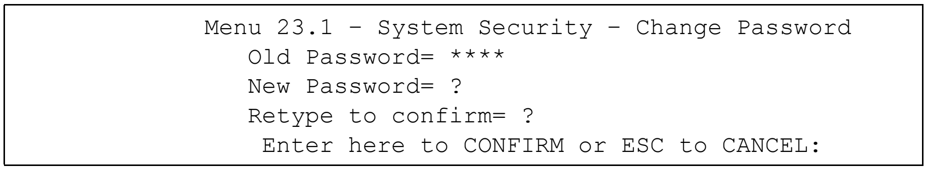
Change the ZyAIR default password by following the steps shown next.

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 69   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.

11.3 ZyAIR SMT Menus Overview

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

Table 36   SMT Menus 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	
14 Dial-in User Setup	14.1 Edit Dial-in User		
16 VLAN Setup			
22 SNMP Configuration			
23 System Security	23.1 Change Password		
	23.2 RADIUS Server		
	23.4 IEEE 802.1X		

Table 36 SMT Menus Overview (continued)

MENUS	SUB MENUS		
24 System Maintenance	24.1 Status		
	24.2 System Information and Console Port Speed	24.2.1 Information	
		24.2.2 Change Console Port Speed	
	24.3 Log and Trace	24.3.1 View Error Log	
	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 Control		

11.4 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 37 Main Menu Commands

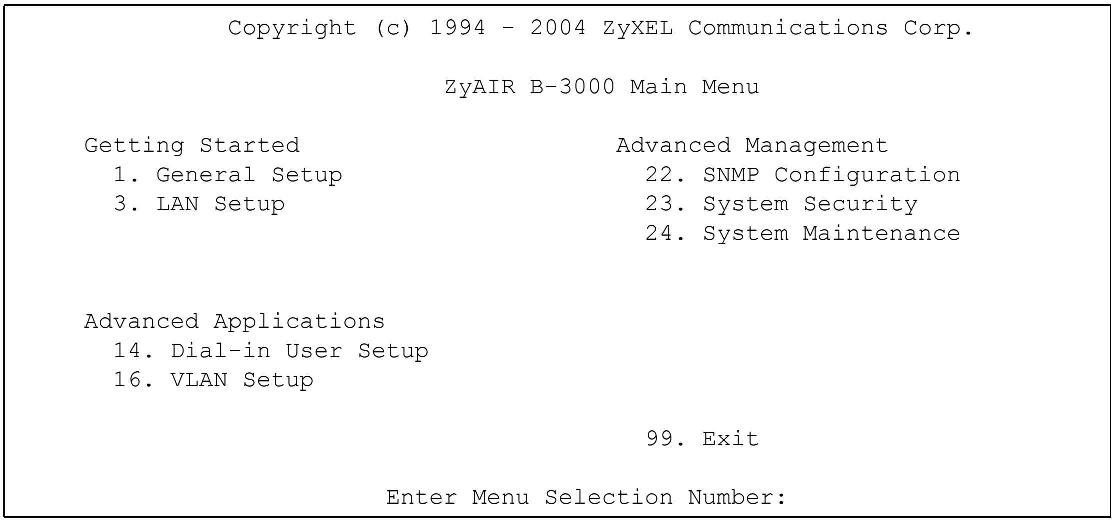
OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change **No** to **Yes** 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 37 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 70 ZyAIR B-3000 SMT Main Menu



```
               Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

                              ZyAIR B-3000 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:
```

11.4.1 System Management Terminal Interface Summary

Table 38 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 ID.
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 38 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 12
General Setup

The chapter shows you the information on general setup.

12.1 General Setup

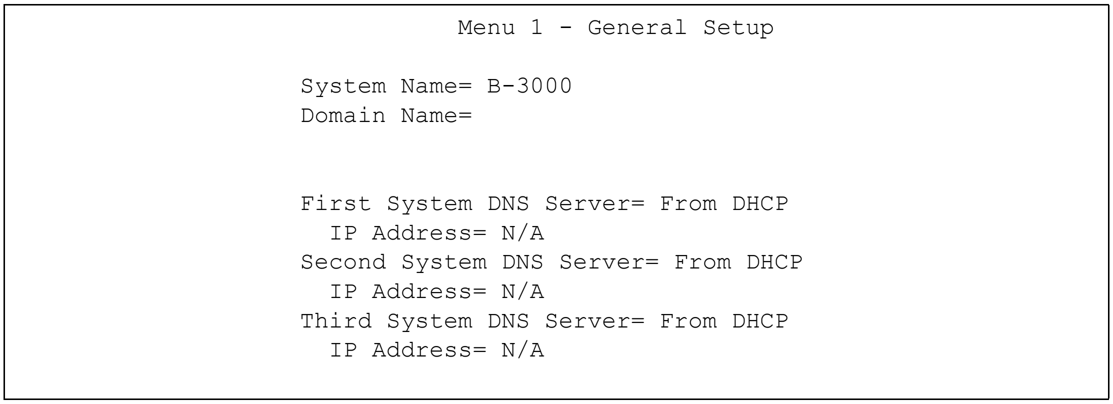
Menu 1 – General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. It is recommended you type your computer's "Computer name".

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.

12.1.1 Procedure To Configure Menu 1

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

Figure 71 Menu 1 General Setup



```
                              Menu 1 - General Setup

                    System Name= B-3000
                    Domain Name=


                    First System DNS Server= From DHCP
                      IP Address= N/A
                    Second System DNS Server= From DHCP
                      IP Address= N/A
                    Third System DNS Server= From DHCP
                      IP Address= N/A
```

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

Table 39 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.
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.	

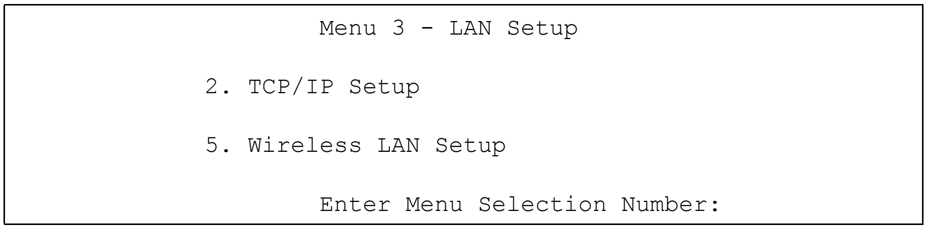
CHAPTER 13
LAN Setup

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

13.1 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 72 Menu 3 LAN Setup



```
                      Menu 3 - LAN Setup

              2. TCP/IP Setup

              5. Wireless LAN Setup

                      Enter Menu Selection Number:
```

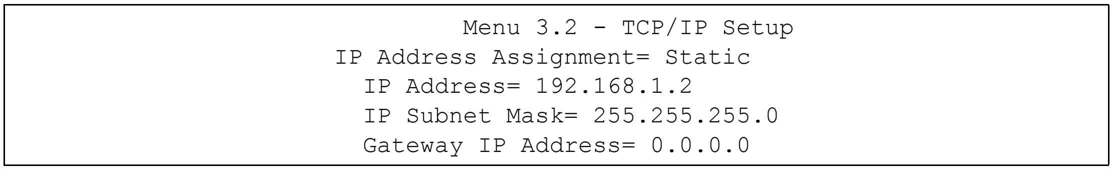
Detailed explanation about the LAN Setup menu is given in the next chapter.

13.2 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 73 Menu 3.2 TCP/IP Setup



```
                                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
```

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

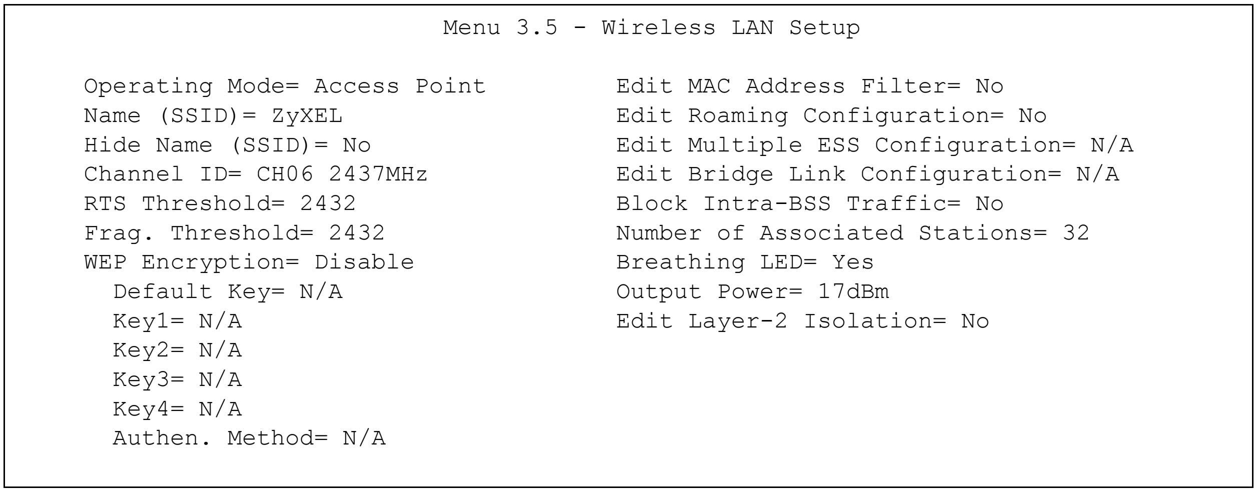
Table 40 Menu 3.2 TCP/IP Setup

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.	

13.3 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 74 Menu 3.5 Wireless LAN Setup



```
                              Menu 3.5 - Wireless LAN Setup

     Operating Mode= Access Point         Edit MAC Address Filter= No
     Name (SSID)= ZyXEL                   Edit Roaming Configuration= No
     Hide Name (SSID)= No                 Edit Multiple ESS Configuration= N/A
     Channel ID= CH06 2437MHz             Edit Bridge Link Configuration= N/A
     RTS Threshold= 2432                  Block Intra-BSS Traffic= No
     Frag. Threshold= 2432                Number of Associated Stations= 32
     WEP Encryption= Disable              Breathing LED= Yes
       Default Key= N/A                   Output Power= 17dBm
       Key1= N/A                          Edit Layer-2 Isolation= No
       Key2= N/A
       Key3= N/A
       Key4= N/A
       Authen. Method= N/A
```

The following table describes the fields in this menu.

Table 41 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
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 passive 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 0 and 2432.
Frag. Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
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.
Default Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the ZyAIR and the wireless stations to communicate.
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** in the **WEP Encryption** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). **Note:** Enter “0x” before the key to denote a hexadecimal key. Don’t enter “0x” before the key to denote an ASCII key.

Table 41 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
Authen. Method	Press [SPACE BAR] to select **Auto**, **Open System Only** or **Shared Key Only** and press [ENTER]. This field is **N/A** if WEP is not activated. If WEP encryption is activated, the default setting is **Auto**.
Edit MAC Address Filter	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.1 - WLAN MAC Address Filter**.
Edit Roaming Configuration	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 3.5.2 - Roaming Configuration**.
Edit Multiple ESS Configuration	Use [SPACE BAR] to choose **Yes** and press [ENTER] to go to **Menu 3.5.3 - Multiple ESS Configuration**.
Edit Bridge Link Configuration	Use [SPACE BAR] to choose **Yes** and press [ENTER] to go to **Menu 3.5.4 - Bridge Link Configuration**.
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.
Number of Association Stations	Enter the number of association stations. The number should be from 1 to 32.
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.
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. Press [SPACE BAR] to select **11dBm**, **13dBm**, **15dBm** or **17dBm** and press [ENTER].
Edit Layer 2 Isolation	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.	

13.3.1 Configuring MAC Address Filter

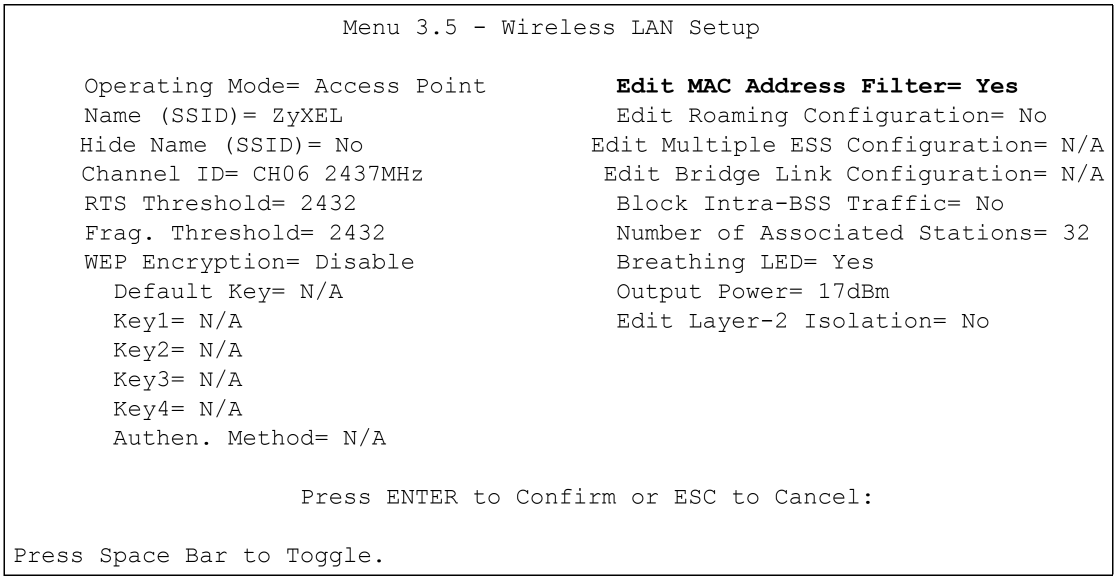
Your ZyAIR checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

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**.

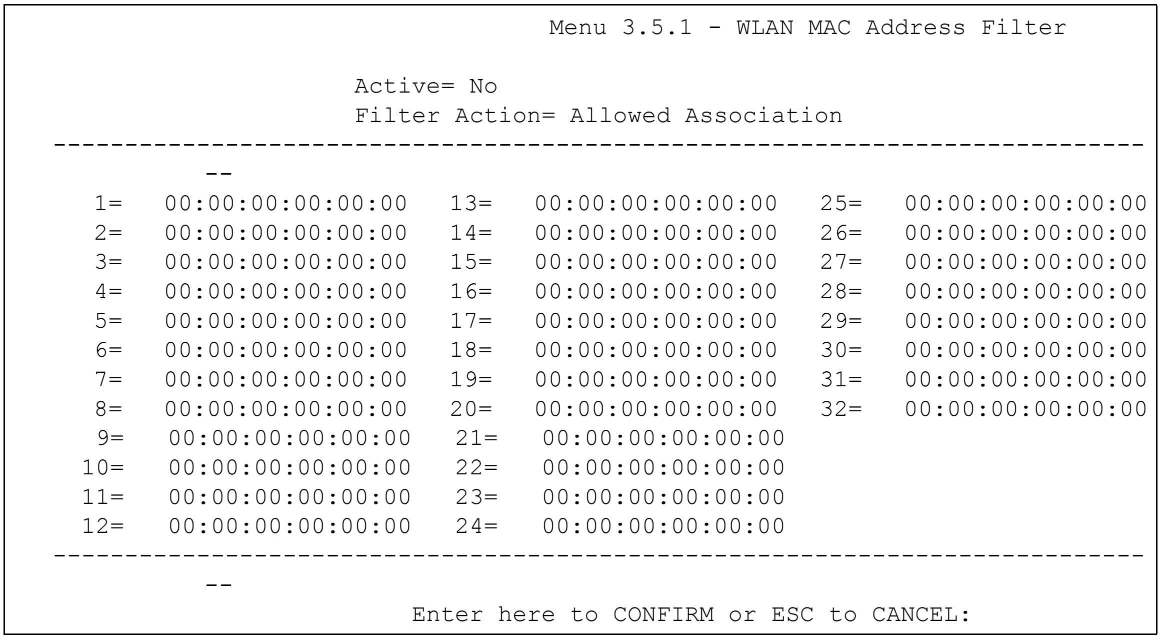
Figure 75 Menu 3.5 Wireless LAN Setup



```
                      Menu 3.5 - Wireless LAN Setup

    Operating Mode= Access Point          Edit MAC Address Filter= Yes
    Name (SSID)= ZyXEL                    Edit Roaming Configuration= No
    Hide Name (SSID)= No                 Edit Multiple ESS Configuration= N/A
    Channel ID= CH06 2437MHz              Edit Bridge Link Configuration= N/A
    RTS Threshold= 2432                   Block Intra-BSS Traffic= No
    Frag. Threshold= 2432                 Number of Associated Stations= 32
    WEP Encryption= Disable               Breathing LED= Yes
      Default Key= N/A                    Output Power= 17dBm
      Key1= N/A                           Edit Layer-2 Isolation= No
      Key2= N/A
      Key3= N/A
      Key4= N/A
      Authen. Method= N/A

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

3 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 76 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 42 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.	

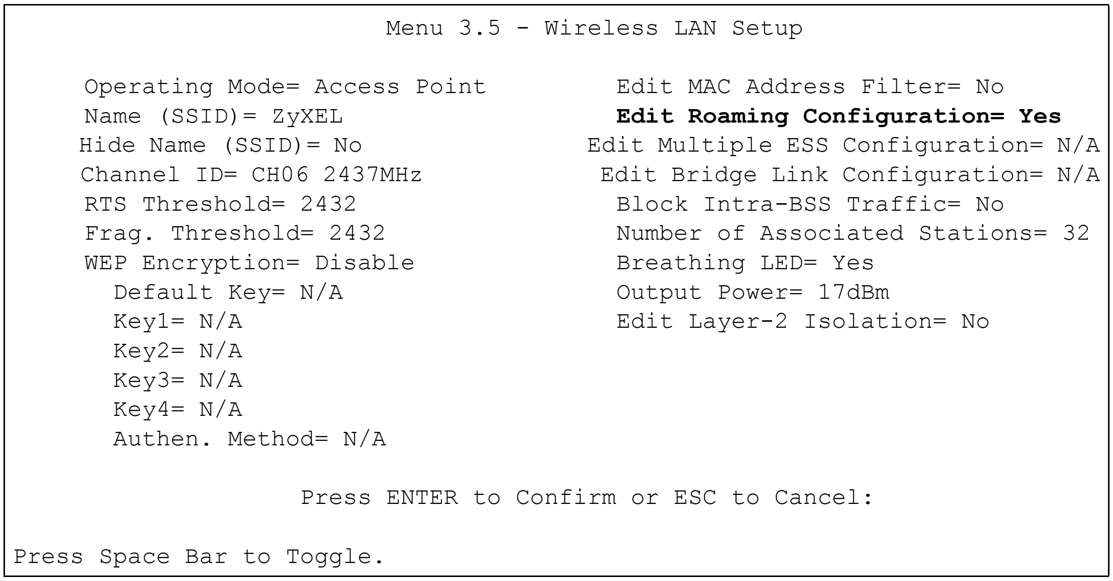
13.3.2 Configuring Roaming

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**.

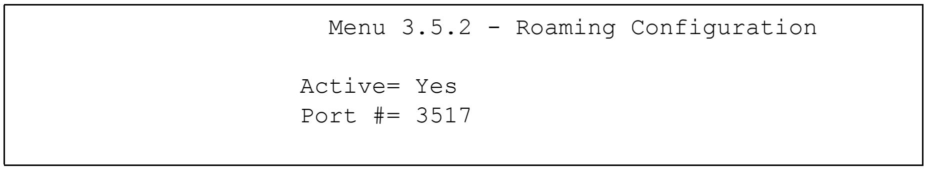
Figure 77 Menu 3.5 Wireless LAN Setup



```
                          Menu 3.5 - Wireless LAN Setup

     Operating Mode= Access Point         Edit MAC Address Filter= No
     Name (SSID)= ZyXEL                   Edit Roaming Configuration= Yes
     Hide Name (SSID)= No               Edit Multiple ESS Configuration= N/A
     Channel ID= CH06 2437MHz            Edit Bridge Link Configuration= N/A
     RTS Threshold= 2432                  Block Intra-BSS Traffic= No
     Frag. Threshold= 2432                Number of Associated Stations= 32
     WEP Encryption= Disable              Breathing LED= Yes
       Default Key= N/A                   Output Power= 17dBm
       Key1= N/A                          Edit Layer-2 Isolation= No
       Key2= N/A
       Key3= N/A
       Key4= N/A
       Authen. Method= N/A

                    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 78 WLAN Roaming Configuration



```
                      Menu 3.5.2 - Roaming Configuration

                    Active= Yes
                    Port #= 3517
```

The following table describes the fields in this menu.

Table 43 Menu 3.5.4 Bridge Link 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.	

CHAPTER 14 Dial-in User Setup

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

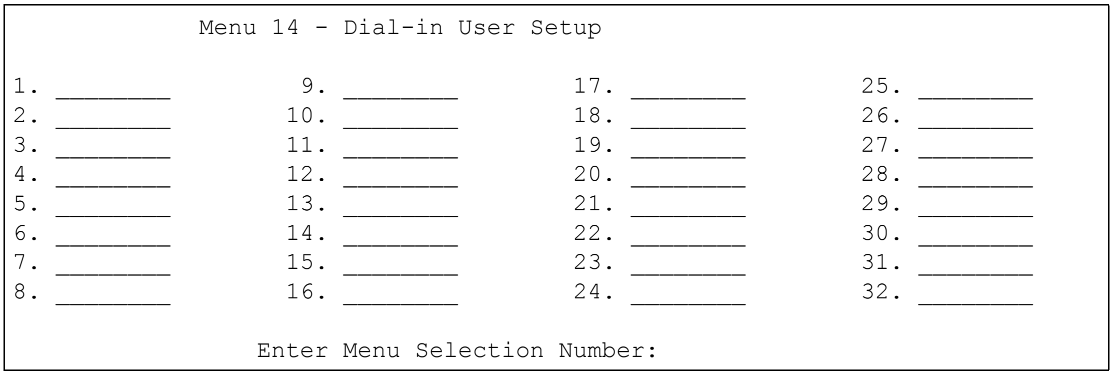
14.1 Dial-in User Setup

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**.

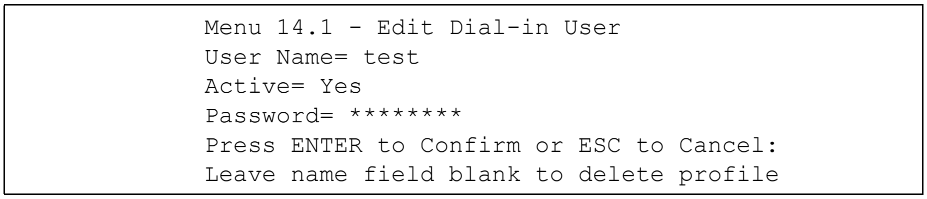
Figure 79 Menu 14- Dial-in User Setup



```
                  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 80   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 44   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.	

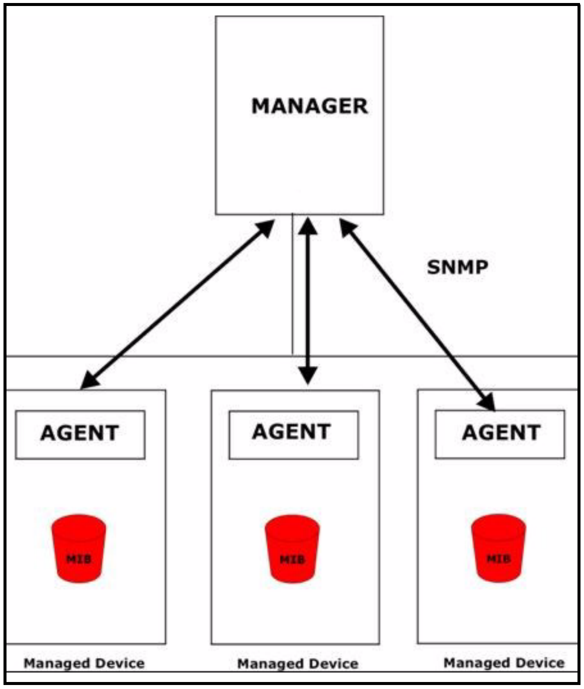
CHAPTER 15 SNMP Configuration

This chapter explains SNMP Configuration menu 22.

15.1 About 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). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 81 SNMP Management Model



An SNMP managed network consists of two main components: 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 the 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.

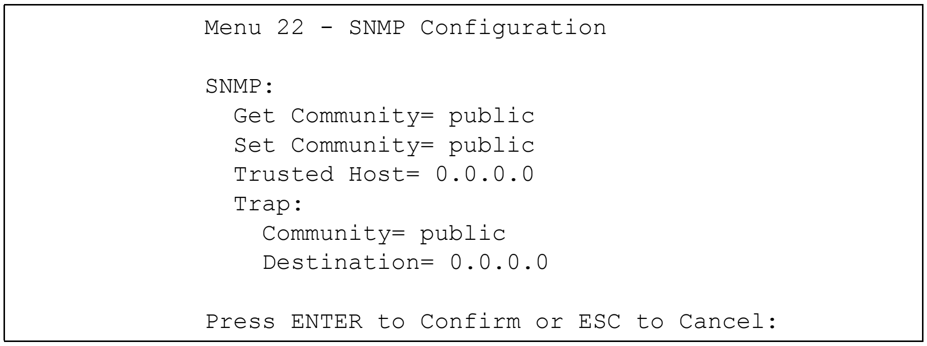
15.2 Supported MIBs

The ZyAIR supports RFC-1215 and MIB II as defined in RFC-1213. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

15.3 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 82 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 45 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.
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.	

15.4 SNMP Traps

The ZyAIR will send traps to the SNMP manager when any one of the following events occurs:

Table 46 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkUp (*defined in RFC-1215*)	A trap is sent when the port is up.

Table 46 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
4	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (*defined in RFC-1215*)	A trap is sent when the port is down.

The following table maps the physical port and encapsulation to the interface type,

Table 47 Ports and Interface Types

PHYSICAL PORT/ENCAP	INTERFACE TYPE
WLAN 1	enet0
Ethernet port	enet1

CHAPTER 16
System Security

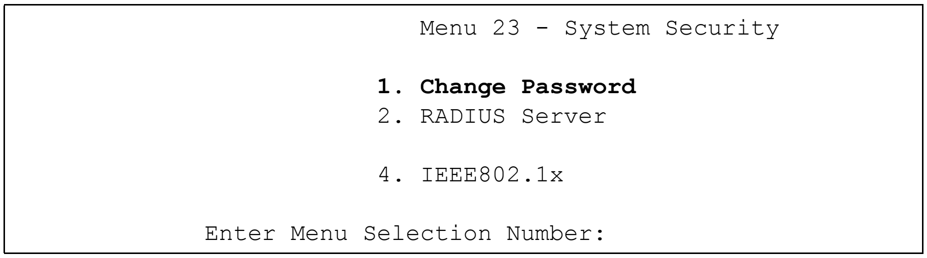
This chapter describes how to configure the system security on the ZyAIR.

16.1 System Security

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

16.1.1 System Password

Figure 83 Menu 23 System Security



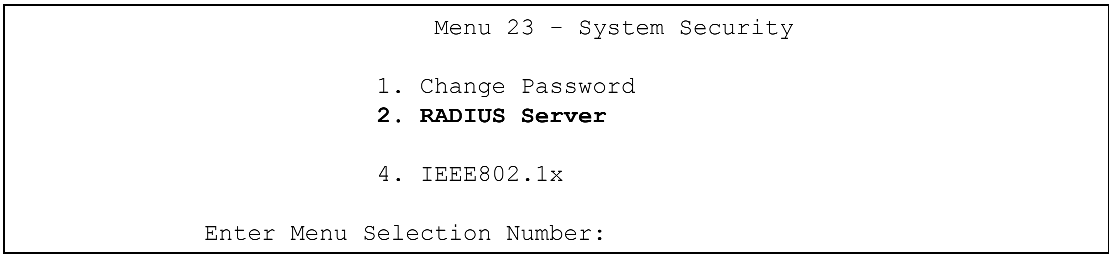
```
                            Menu 23 - System Security

                         1. Change Password
                         2. RADIUS Server

                         4. IEEE802.1x

              Enter Menu Selection Number:
```

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.

16.1.2 Configuring External RADIUS Server

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

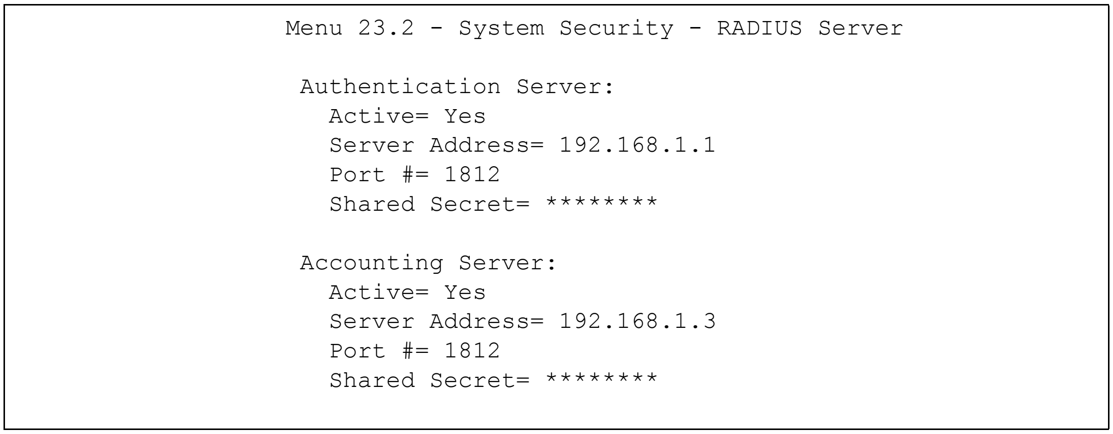
Figure 84 Menu 23 System Security



```
                             Menu 23 - System Security

                         1. Change Password
                         2. RADIUS Server

                         4. IEEE802.1x

                 Enter Menu Selection Number:
```

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 – System Security – RADIUS Server** as shown next.

Figure 85 Menu 23.2 System Security : RADIUS Server



```
                  Menu 23.2 - System Security - RADIUS Server

                   Authentication Server:
                     Active= Yes
                     Server Address= 192.168.1.1
                     Port #= 1812
                     Shared Secret= ********

                   Accounting Server:
                     Active= Yes
                     Server Address= 192.168.1.3
                     Port #= 1812
                     Shared Secret= ********
```

The following table describes the fields in this menu.

Table 48 Menu 23.2 System Security : RADIUS Server

FIELD	DESCRIPTION
Authentication Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and ZyAIR.
Accounting Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server.

Table 48 Menu 23.2 System Security : RADIUS Server

FIELD	DESCRIPTION
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and 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.	

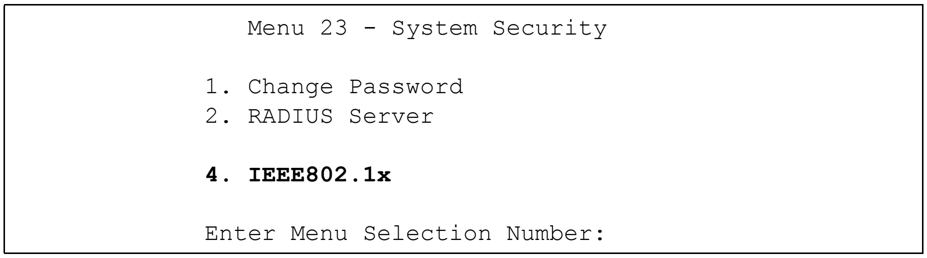
16.1.3 802.1x

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

Follow the steps below to enable EAP authentication on your ZyAIR.

1 From the main menu, enter 23 to display **Menu23 – System Security**.

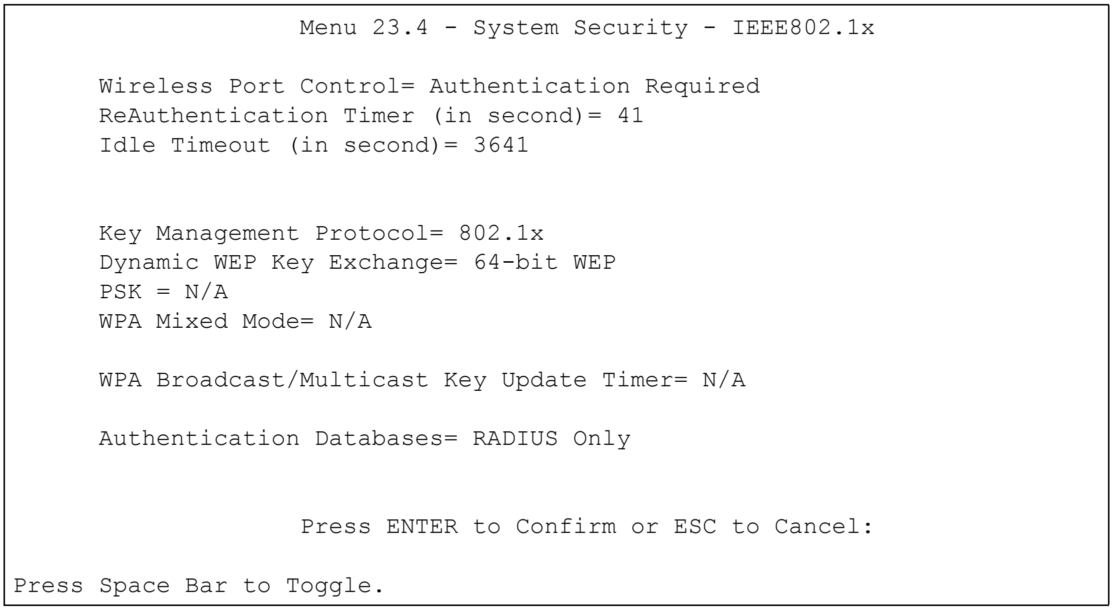
Figure 86 Menu 23 System Security



```
                Menu 23 - System Security

             1. Change Password
             2. RADIUS Server

             4. IEEE802.1x

             Enter Menu Selection Number:
```

2 Enter 4 to display **Menu 23.4 – System Security – IEEE802.1x**.

Figure 87 Menu 23.4 System Security : IEEE802.1x



```
                    Menu 23.4 - System Security - IEEE802.1x

      Wireless Port Control= Authentication Required
      ReAuthentication Timer (in second)= 41
      Idle Timeout (in second)= 3641


      Key Management Protocol= 802.1x
      Dynamic WEP Key Exchange= 64-bit WEP
      PSK = N/A
      WPA Mixed Mode= N/A

      WPA Broadcast/Multicast Key Update Timer= N/A

      Authentication Databases= RADIUS Only


                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The following table describes the fields in this menu.

Table 49 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	Press [SPACE BAR] and select a security mode for the wireless LAN access. Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting. Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **No Access Allowed** to block all wireless stations access to the wired network. The following fields are not available when you select **No Authentication Required** or **No Access Allowed**.
ReAuthentication Timer (in second)	Specify how often a client has to re-enter username and password to stay connected to the wired network. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is **1800** seconds (or 30 minutes).
Idle Timeout (in second)	The ZyAIR automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).
Key Management Protocol	Press [SPACE BAR] to select **802.1x**, **WPA** or **WPA-PSK** and press [ENTER].

Table 49 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the ZyAIR when you configure Dynamic WEP Key Exchange.
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select **WPA-PSK** in the **Key Management Protocol** field.
WPA Mixed Mode	Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable** and configure **Data Privacy for Broadcast/Multicast packets** field.
WPA Broadcast/ Multicast Key Update Timer	The **WPA Broadcast/Multicast 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 **WPA Broadcast/ Multicast Key Update Timer** is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).
Authentication Databases	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 field to decide which database the ZyAIR should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database** with **802.1x Key Management Protocol**. 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. 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. 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. 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.
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.	

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the ZyAIR for authentication

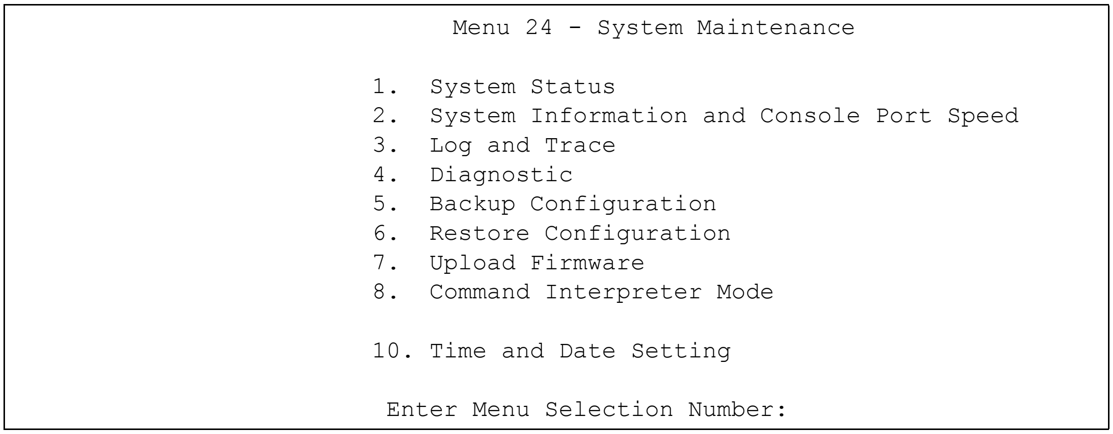
Chapter 17 System Information and Diagnosis

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 88 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

                          Enter Menu Selection Number:
```

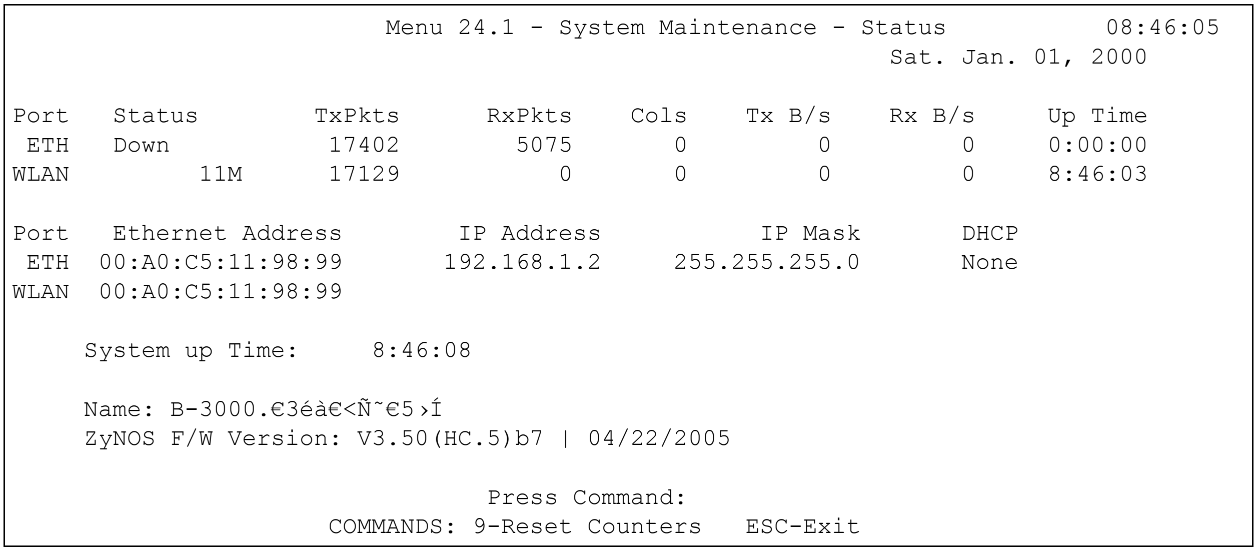
17.1 System Status

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 89   Menu 24.1 System Maintenance : Status



```
                          Menu 24.1 - System Maintenance - Status          08:46:05
                                                               Sat. Jan. 01, 2000

Port   Status        TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
 ETH   Down           17402        5075       0         0         0     0:00:00
WLAN        11M       17129           0       0         0         0     8:46:03

Port   Ethernet Address        IP Address          IP Mask       DHCP
 ETH  00:A0:C5:11:98:99       192.168.1.2     255.255.255.0       None
WLAN  00:A0:C5:11:98:99

     System up Time:     8:46:08

     Name: B-3000.€3éà€<Ñ˜€5›Í
     ZyNOS F/W Version: V3.50(HC.5)b7 | 04/22/2005

                                 Press Command:
                      COMMANDS: 9-Reset Counters   ESC-Exit
```

The following table describes the fields present in this menu.

Table 50   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.

17.2 System Information

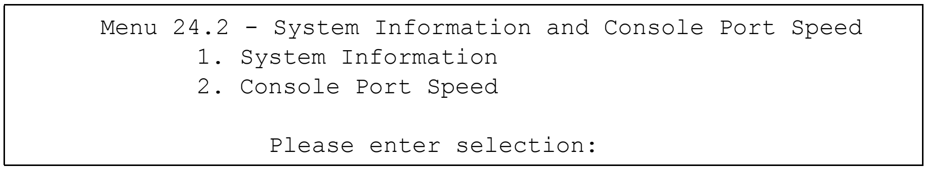
To get to the System Information:

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 90 Menu 24.2 System Information and Console Port Speed



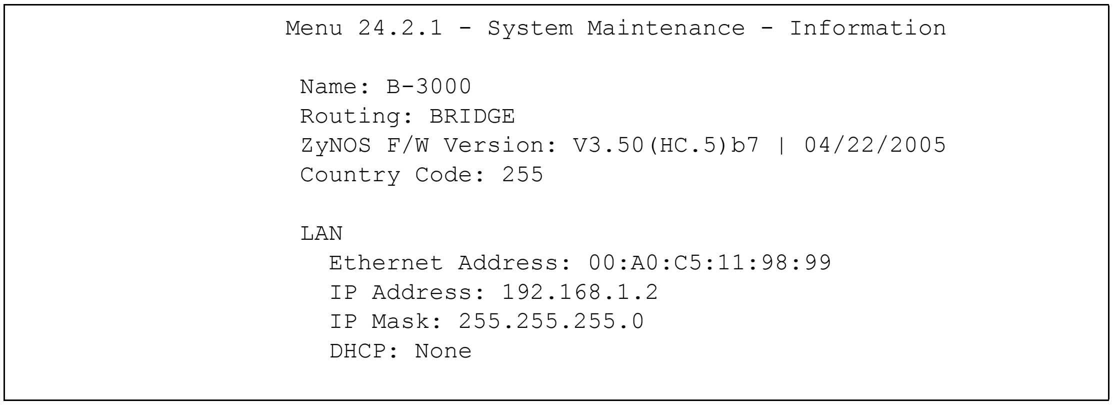
```
     Menu 24.2 - System Information and Console Port Speed
            1. System Information
            2. Console Port Speed

                 Please enter selection:
```

Note: The console port is internal and reserved for technician use only.

17.2.1 System Information

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

Figure 91 Menu 24.2.1 System Information : Information



```
                    Menu 24.2.1 - System Maintenance - Information

                     Name: B-3000
                     Routing: BRIDGE
                     ZyNOS F/W Version: V3.50(HC.5)b7 | 04/22/2005
                     Country Code: 255

                     LAN
                       Ethernet Address: 00:A0:C5:11:98:99
                       IP Address: 192.168.1.2
                       IP Mask: 255.255.255.0
                       DHCP: None
```

The following table describes the fields in this menu.

Table 51 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.
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.

Table 51 Menu 24.2.1 System Maintenance : Information

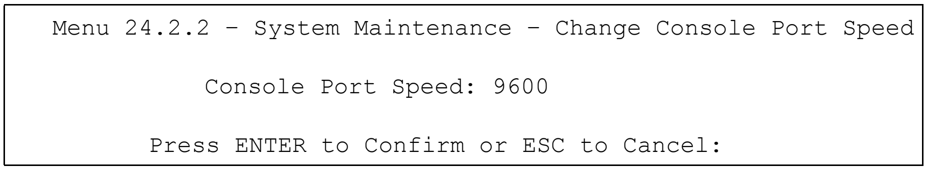
FIELD	DESCRIPTION
IP Address	This is the IP address of the ZyAIR in dotted decimal notation.
IP Mask	This shows the subnet mask of the ZyAIR.
DHCP	This field shows the DHCP setting of the ZyAIR.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

17.2.2 Console Port Speed

Note: The console port is internal and reserved for technician use only.

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 92 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.

17.3 Log and Trace

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

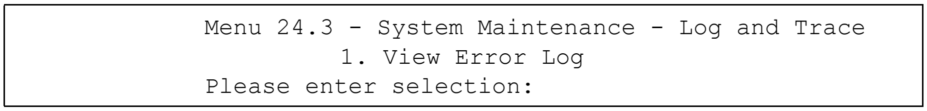
17.3.1 Viewing Error Log

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 93 Menu 24.3 System Maintenance : Log and Trace

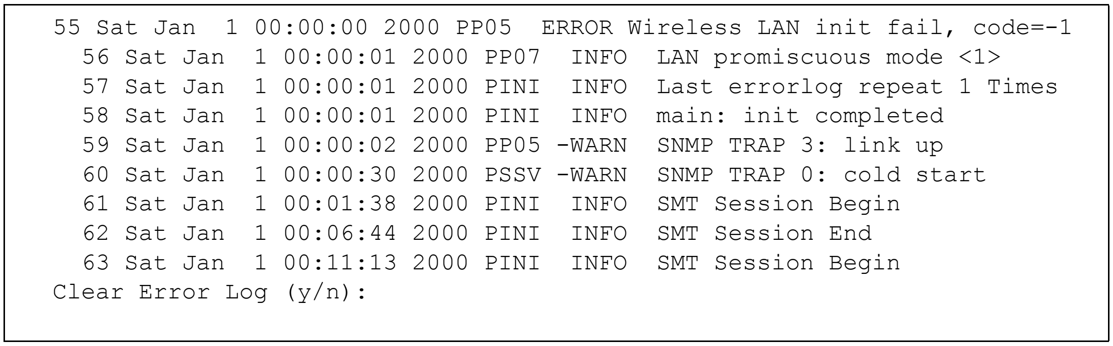


```
              Menu 24.3 - System Maintenance - Log and Trace
                        1. View Error Log
              Please enter selection:
```

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 94 Sample Error and Information Messages

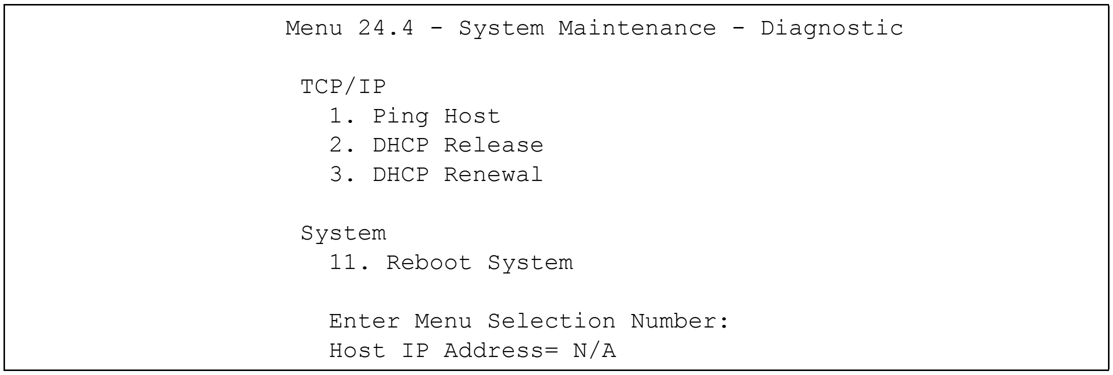


```
 55 Sat Jan  1 00:00:00 2000 PP05  ERROR Wireless LAN init fail, code=-1
   56 Sat Jan  1 00:00:01 2000 PP07  INFO  LAN promiscuous mode <1>
   57 Sat Jan  1 00:00:01 2000 PINI  INFO  Last errorlog repeat 1 Times
   58 Sat Jan  1 00:00:01 2000 PINI  INFO  main: init completed
   59 Sat Jan  1 00:00:02 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):
```

17.4 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 95 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 52 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 18 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.

18.1 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 53 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.

18.2 Backup Configuration

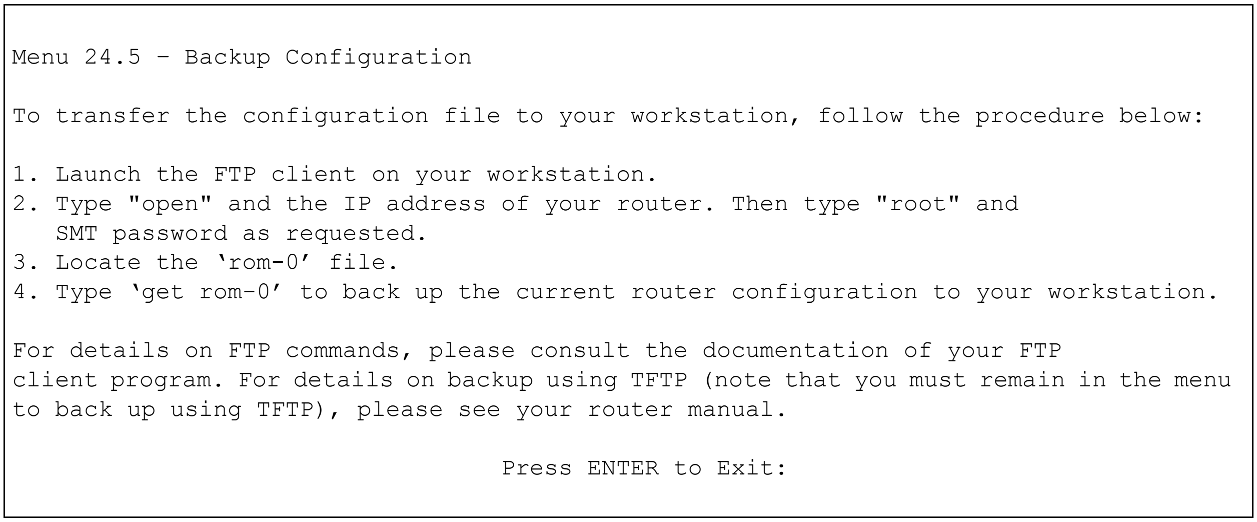
Option 5 from **Menu 24 – System Maintenance** allows you to backup the current ZyAIR configuration to your computer. Backup is highly recommended once your ZyAIR is functioning properly. FTP is the preferred method, although TFTP can also be used.

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.

18.2.1 Backup Configuration Using FTP

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

Figure 96 Menu 24.5 Backup Configuration



```
Menu 24.5 - Backup Configuration

To transfer the configuration file to your workstation, 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. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to your workstation.

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

                                  Press ENTER to Exit:
```

18.2.2 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.

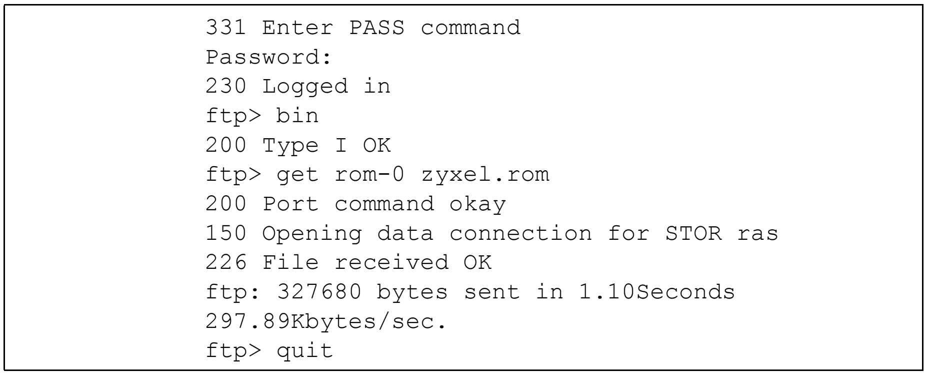
4 Enter "root" and your SMT password as requested. The default is 1234.

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 97 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 54 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).

18.2.3 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.

18.2.4 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 55 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.

18.2.5 Backup Via Console Port

Note: The console port is internal and reserved for technician use only.

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 98 System Maintenance: Backup Configuration

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

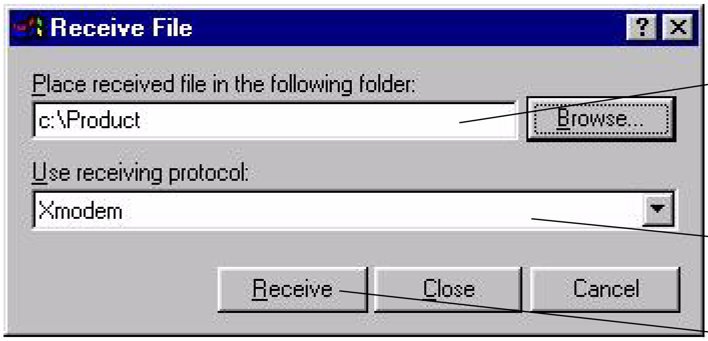
2 The following screen indicates that the Xmodem download has started.

Figure 99 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 100 Backup Configuration Example



Receive File

Place received file in the following folder: c:\Product

Use receiving protocol: Xmodem

Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

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

Figure 101 Successful Backup Confirmation Screen

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

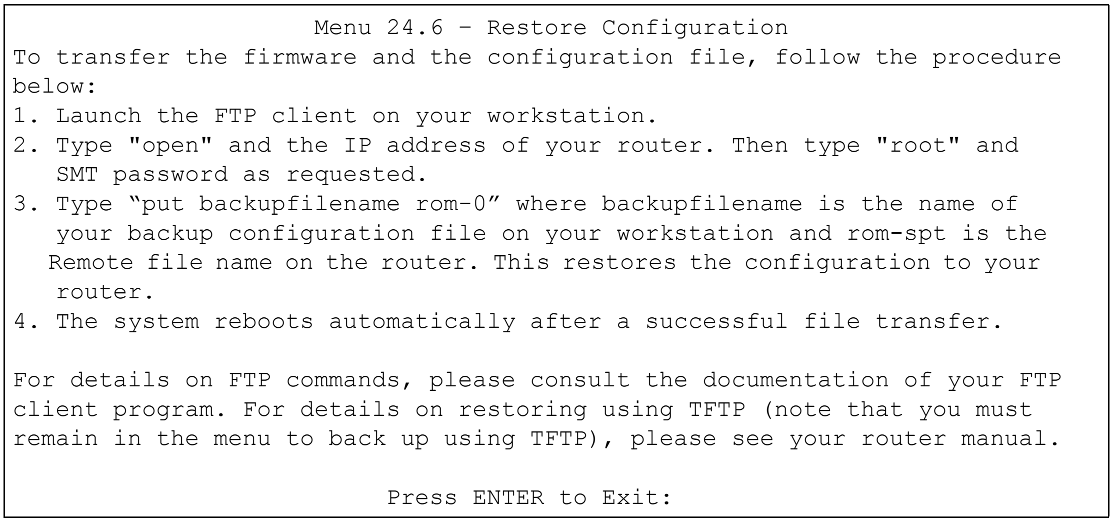
18.3 Restore Configuration

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.

18.3.1 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 102 Menu 24.6 Restore Configuration



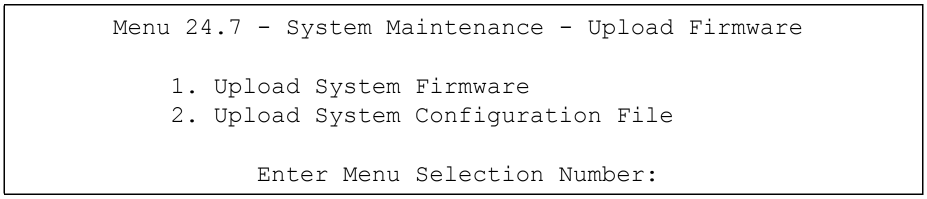
```
                     Menu 24.6 - Restore Configuration
To transfer the firmware and the configuration file, follow the procedure
below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type “put backupfilename 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:
```

18.4 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 103 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:
```

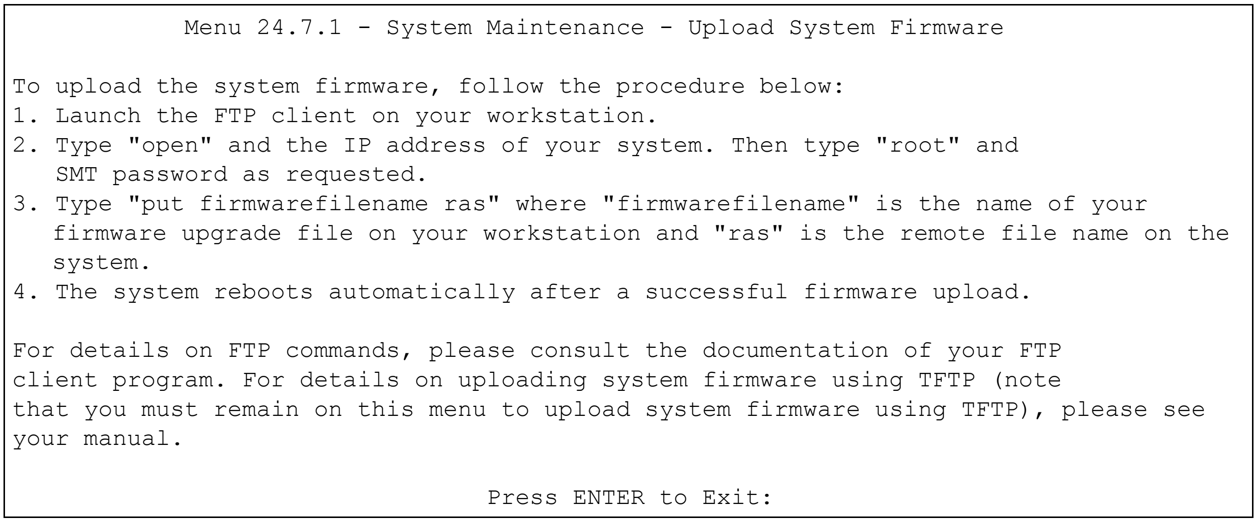
The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

18.4.1 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 104 Menu 24.7.1 System Maintenance : Upload System Firmware

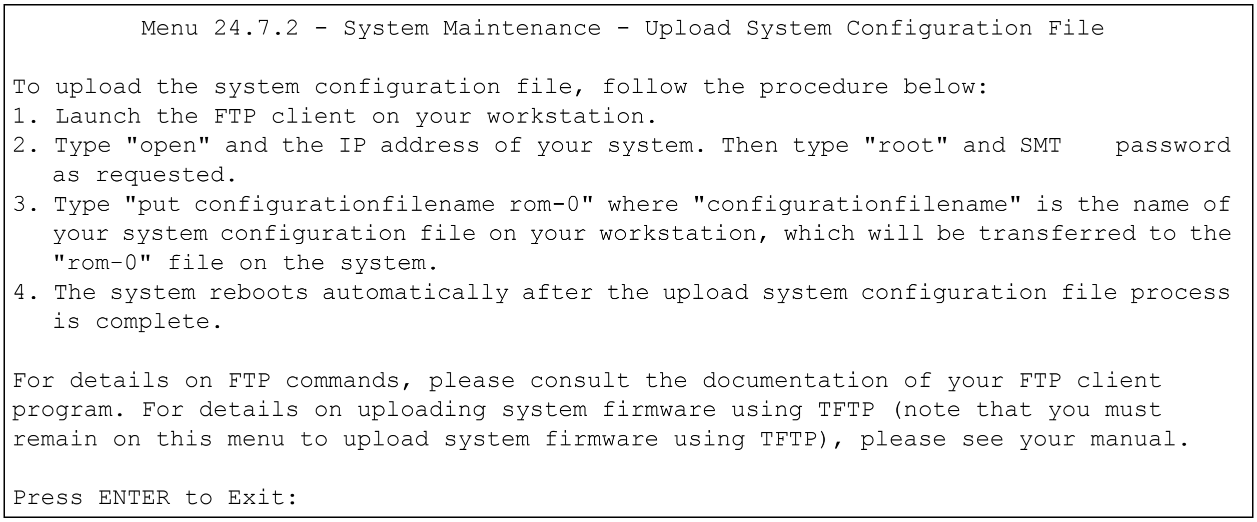


```
            Menu 24.7.1 - System Maintenance - Upload System Firmware

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:
```

18.4.2 Configuration File Upload

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

Figure 105 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:

18.4.3 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 106 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.

18.4.4 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.

18.4.5 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.

18.4.6 Uploading Via Console Port

Note: The console port is internal and reserved for technician use only.

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.

18.4.7 Uploading Firmware File Via Console Port

Note: The console port is internal and reserved for technician use only.

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 107 Menu 24.7.1 as seen using the Console Port

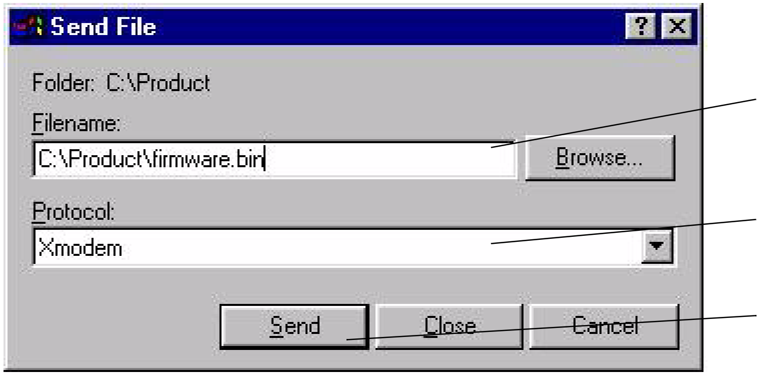
```
              Menu 24.7.1 - System Maintenance - Upload System Firmware
            To upload system firmware:
            1. Enter "y" at the prompt below to go into debug mode.
            2. Enter "atur" after "Enter Debug Mode" message.
            3. Wait for "Starting XMODEM upload" message 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.

18.4.8 Example Xmodem Firmware Upload Using HyperTerminal

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

Figure 108 Example Xmodem Upload



Folder: C:\Product

Filename:
C:\Product\firmware.bin

Protocol:
Xmodem

Type the firmware file’s location, or click **Browse** to look for it.

Choose the **Xmodem** protocol.

Then click **Send**.

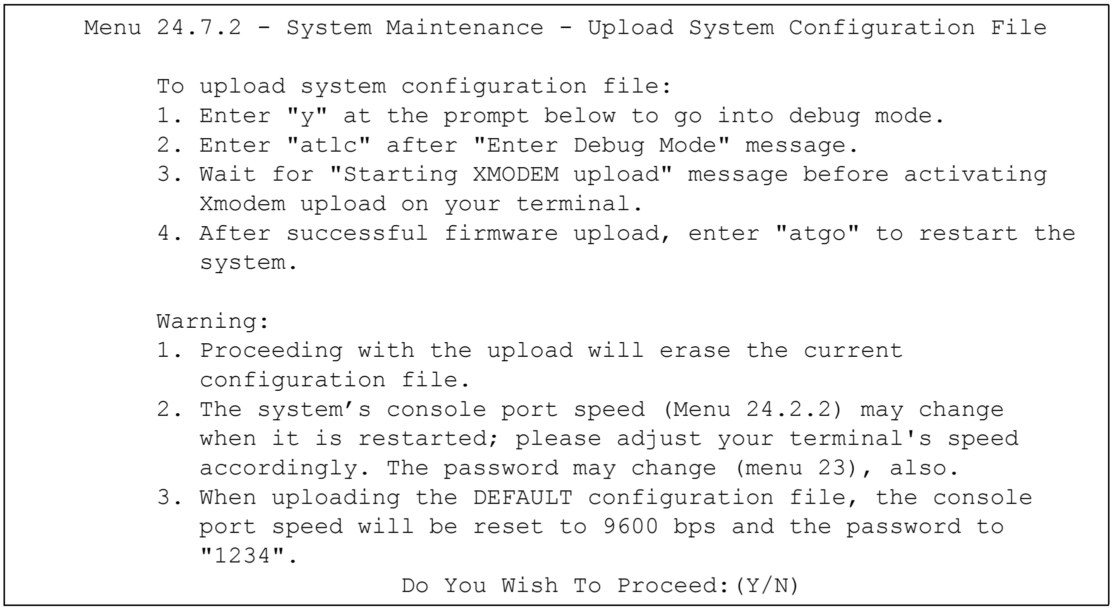
After the firmware upload process has completed, the ZyAIR will automatically restart.

18.4.9 Uploading Configuration File Via Console Port

Note: The console port is internal and reserved for technician use only.

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 109   Menu 24.7.2 as seen using the Console Port



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

          To upload system configuration file:
          1. Enter "y" at the prompt below to go into debug mode.
          2. Enter "atlc" 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
             system.

          Warning:
          1. Proceeding with the upload will erase the current
             configuration file.
          2. The system’s console port speed (Menu 24.2.2) may change
             when it is restarted; please adjust your terminal's speed
             accordingly. The password may change (menu 23), also.
          3. When uploading the DEFAULT configuration file, the console
             port speed will be reset to 9600 bps and the password to
             "1234".
                            Do You Wish To Proceed:(Y/N)
```

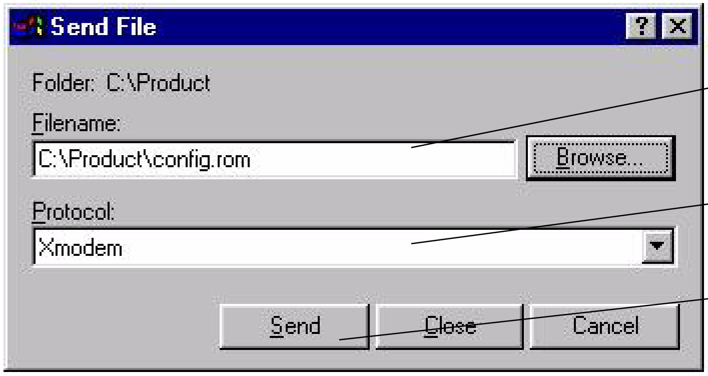
2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter “atgo” to restart the ZyAIR.

18.4.10 Example Xmodem Configuration Upload Using HyperTerminal

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

Figure 110   Example Xmodem Upload



Folder: C:\Product

Filename:
C:\Product\config.rom

Protocol:
Xmodem

Type the configuration file’s location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

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

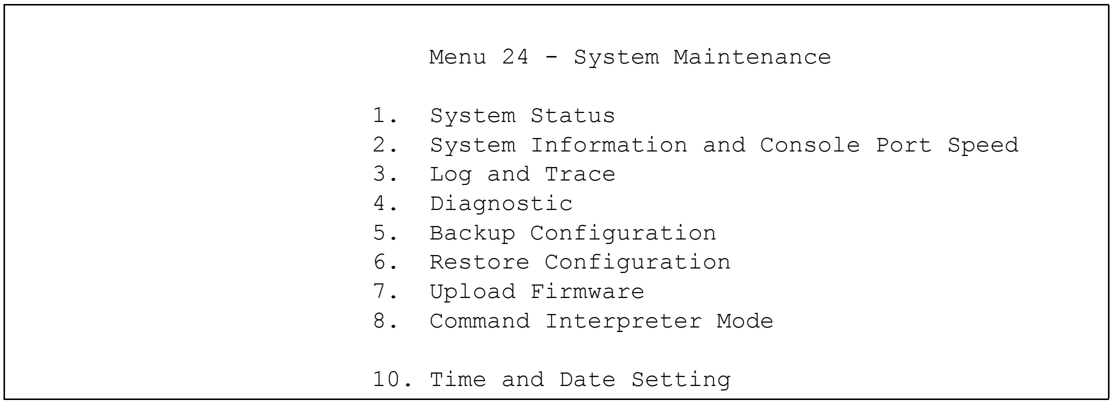
CHAPTER 19 System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

19.1 Command Interpreter Mode

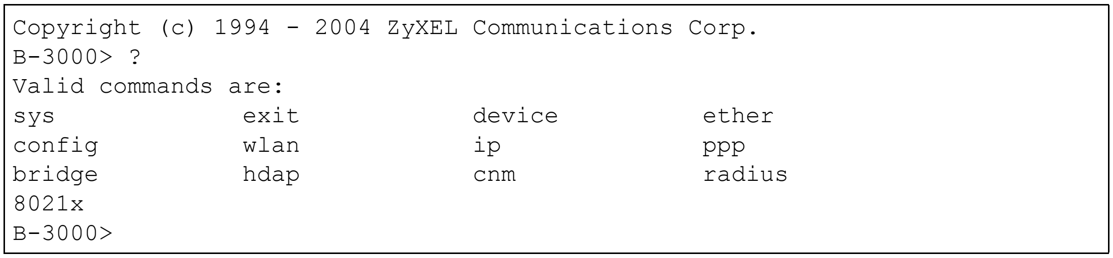
The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed 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 111 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
```

Figure 112 Valid CI Commands



```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
B-3000> ?
Valid commands are:
sys             exit            device          ether
config          wlan            ip              ppp
bridge          hdap            cnm             radius
8021x
B-3000>
```

19.1.1 CNM

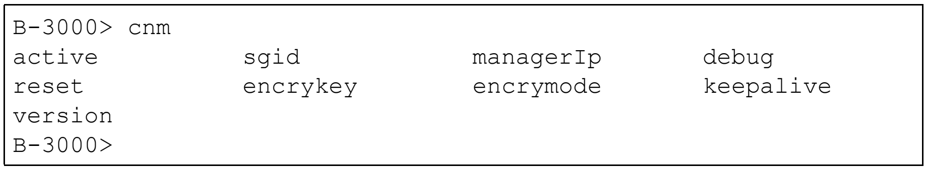
Vantage CNM (Centralized Network Management) is a browser-based, global management solution that allows an administrator to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the Vantage CNM User’s Guide for details.

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

19.1.2 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 113 CNM CL



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

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 56 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 56 CNM Commands

COMMAND	SUB COMMAND	DESCRIPTION
managerIp		This command displays the public IP address of the Vantage CNM server. 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. If the Vantage CNM server is on a different subnet to the ZyXEL device, enter the public IP address of the Vantage CNM server. 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. 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).
	[addr]	Use this command to set the IP address of the Vantage CNM server.
debug	<0:Disable 1:Vantage 2:Agent tester 3:Server>	This command displays the output of Vantage CNM debug messages.
	0	Type this command to not display Vantage CNM debug messages.
	1	Type this command to display Vantage CNM debug messages on the console after the ZyXEL device registers with the Vantage CNM server.
	2	Type this command to display Vantage CNM debug messages on the console after the ZyXEL device registers with the Vantage CNM server.
	3	Type this command to display Vantage CNM debug messages on the console after the ZyXEL device registers with the Vantage CNM server.
reset		Have the ZyXEL device send register request messages to the Vantage CNM server.
encrykey		This displays the encryption key, which is used to encrypt and decrypt messages between Vantage CNM and the device.
	[string]	Use this command to specify the encryption key. Type eight alphanumeric characters when you choose DES encryption algorithm. Type 24 alphanumeric characters when you choose 3DES encryption algorithm. The ZyXEL device must have the same encryption key as the Vantage CNM server.

Table 56 CNM Commands

COMMAND	SUB COMMAND	DESCRIPTION
`encrymode`		This command is used to encrypt communications between the ZyXEL device and the Vantage CNM server. Use this command to set the encryption mode.

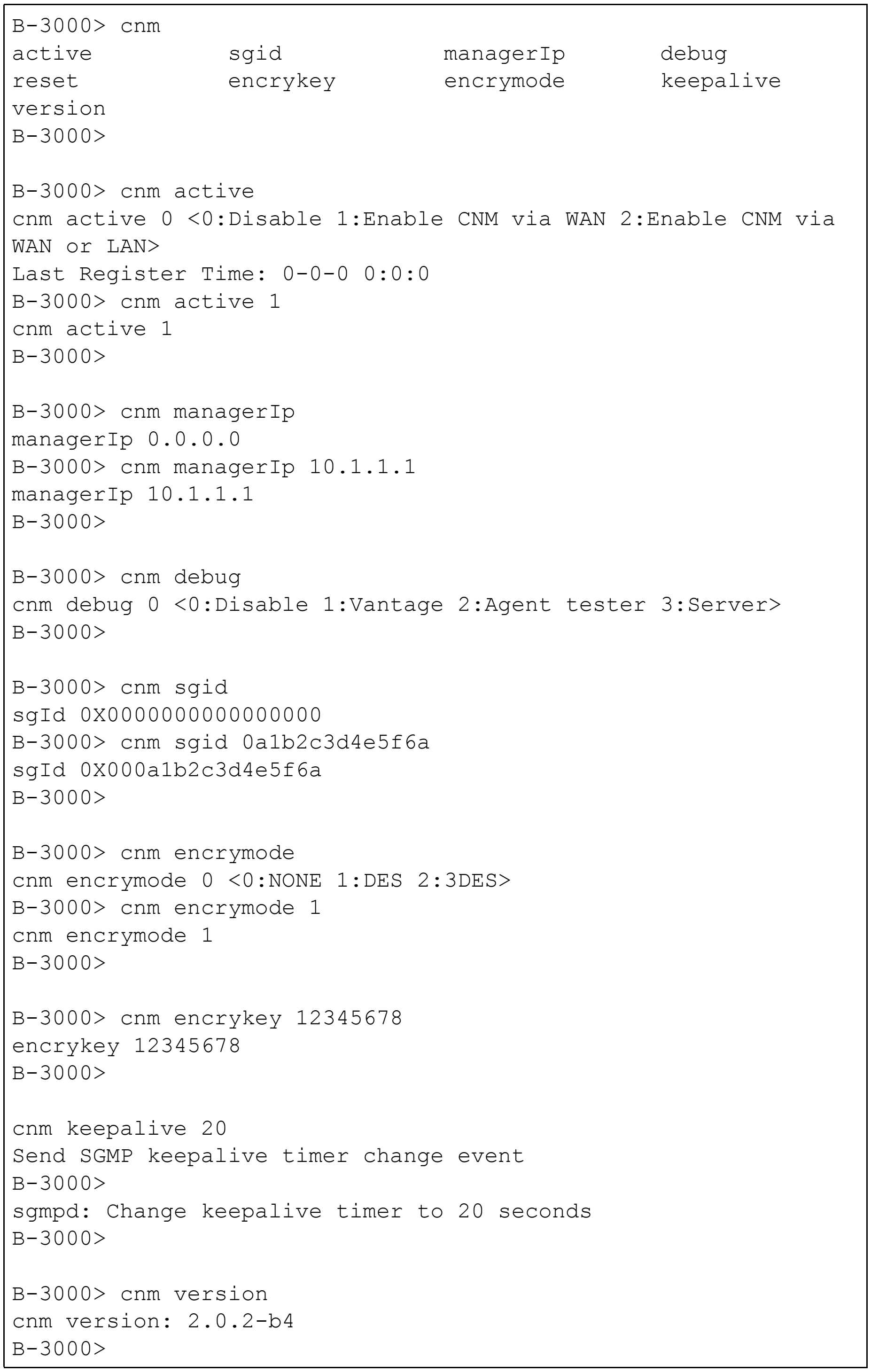
	`<0:NONE`
	`1:DES`
	`2:3DES>`
		Type 0 to have no encryption, type 1 to have the ZyXEL device use DES encryption or type 2 to have the ZyXEL device use 3DES encryption.
		The ZyXEL device must use the same encryption mode as the Vantage CNM server.

keepalive		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.
	0	Use this command to disable keepalive message sending.
	[seconds]	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.

19.1.3 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 114 CNM Configuration Example



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

B-3000> 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
B-3000> cnm active 1
cnm active 1
B-3000>

B-3000> cnm managerIp
managerIp 0.0.0.0
B-3000> cnm managerIp 10.1.1.1
managerIp 10.1.1.1
B-3000>

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

B-3000> cnm sgid
sgId 0X0000000000000000
B-3000> cnm sgid 0a1b2c3d4e5f6a
sgId 0X000a1b2c3d4e5f6a
B-3000>

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

B-3000> cnm encrykey 12345678
encrykey 12345678
B-3000>

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

B-3000> cnm version
cnm version: 2.0.2-b4
B-3000>
```

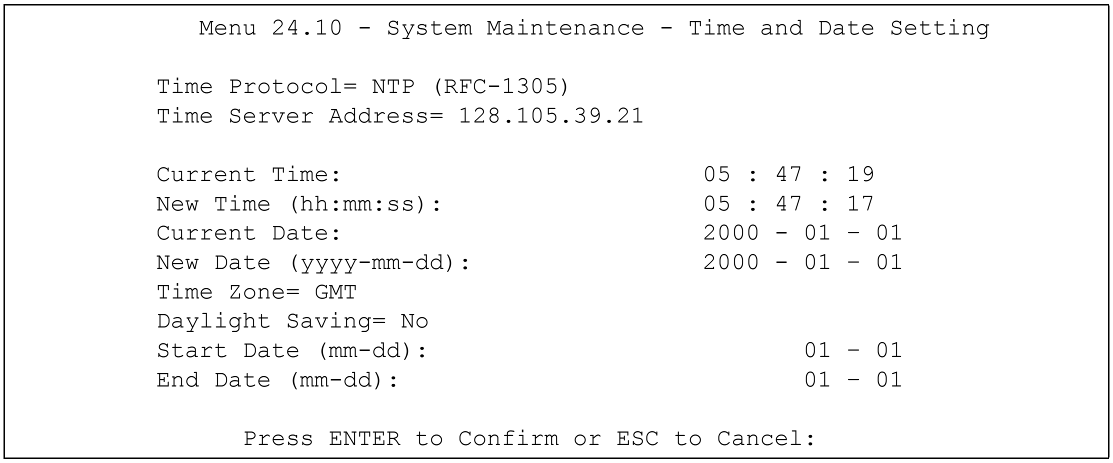
19.2 Time and Date Setting

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 115 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 57 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 57 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.	

19.2.1 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.

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 58 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 59 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 60 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 61 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 62 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 63 Hardware

Power Specification	DC 12V 1200mA
Operation Temperature	5º C ~ 50º C
Storage Temperature	-20º C ~ 55º C
Operation Humidity	10% to 90% (Non-condensing)
Storage Humidity	5% to 95% (Non-condensing)

Firmware

Table 64 Firmware

Standards	IEEE 802.3 and 802.3u 10Base-T and 100Base-TX. IEEE 802.11b 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 64 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.

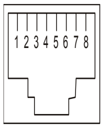
Appendix C
Power over Ethernet Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.-7

Table 65 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Table 66 Power over Ethernet Injector RJ-45 Port Pin Assignments

		**RJ-45 SIGNAL ASSIGNMENT**
		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 67 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.

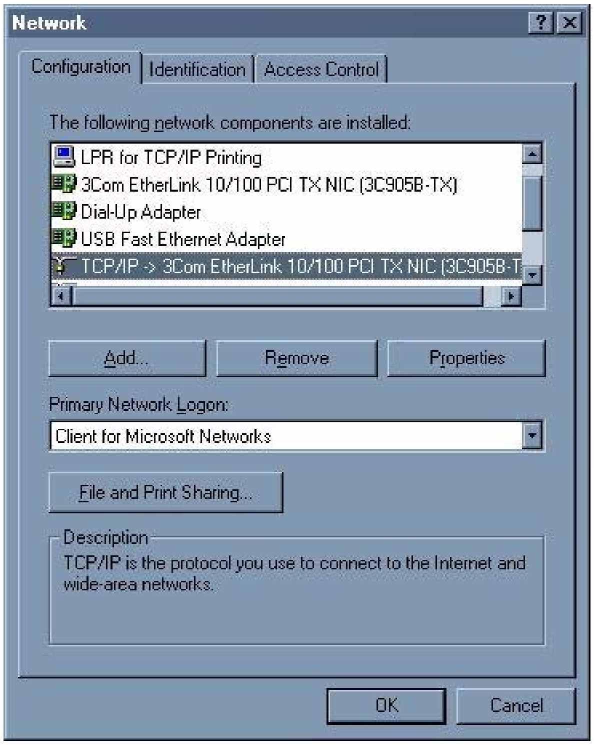
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 116 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

LPR for TCP/IP Printing
3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
Dial-Up Adapter
USB Fast Ethernet Adapter
TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

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.

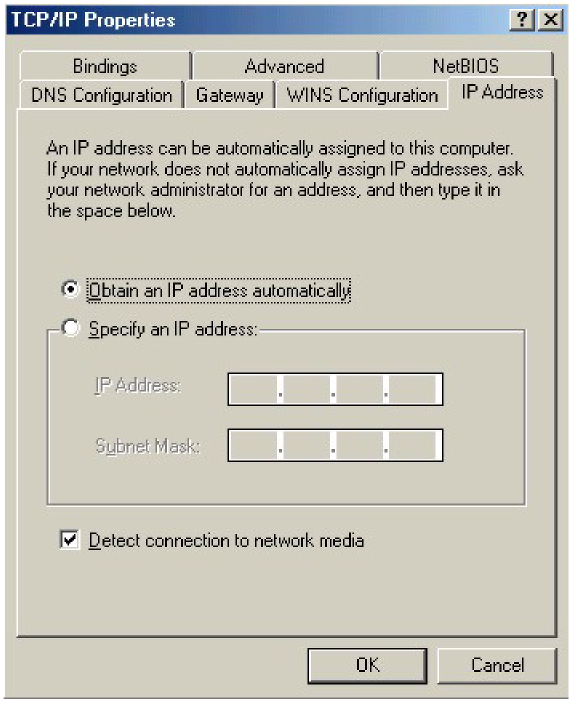
Configuring

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 117 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

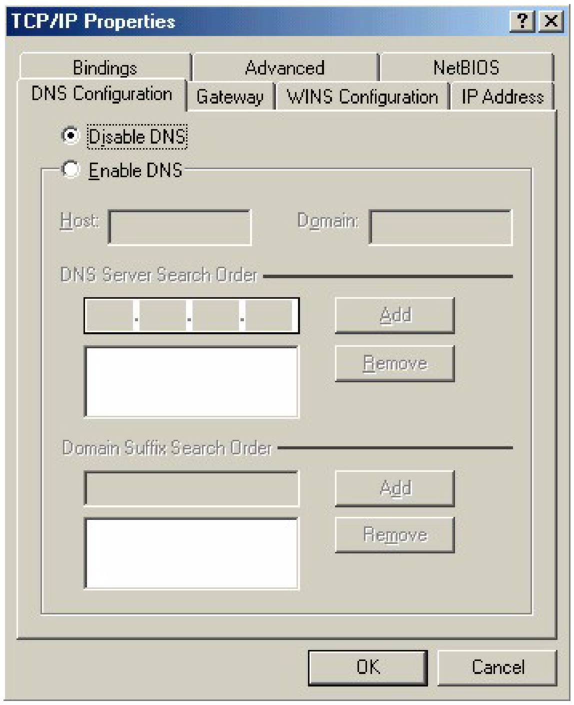
Subnet Mask: . . .

☑ Detect connection to network media

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 118 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

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**.

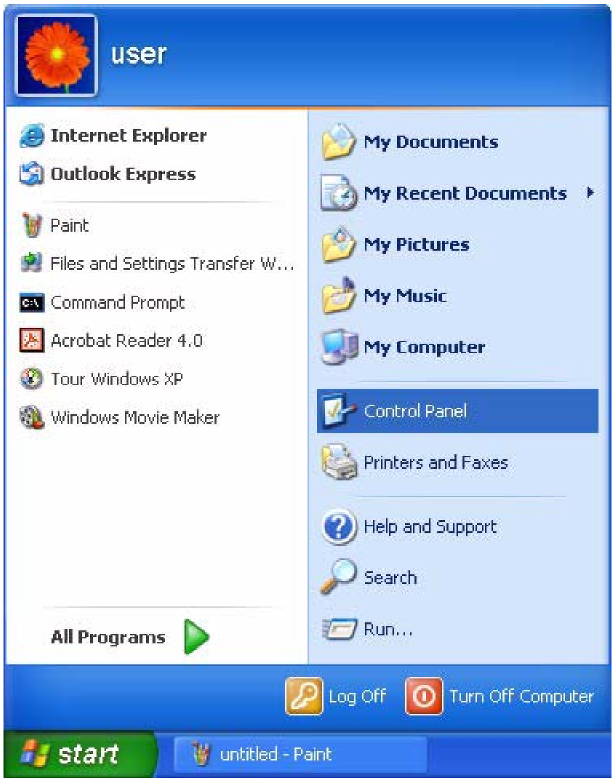
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

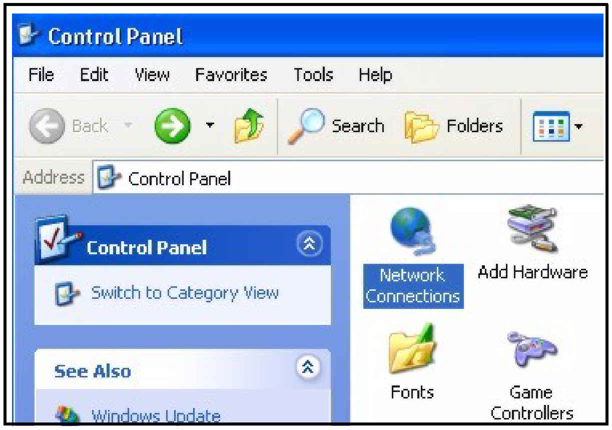
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 119 Windows XP: Start Menu



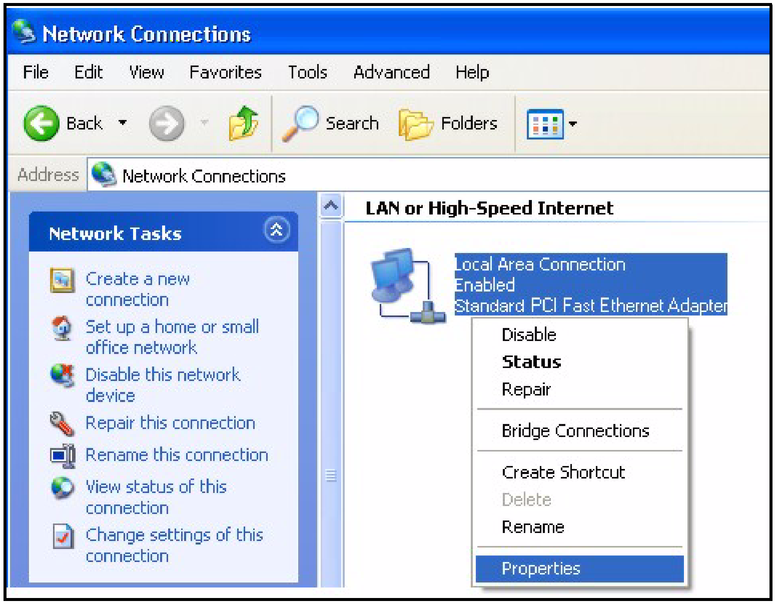
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 120 Windows XP: Control Panel



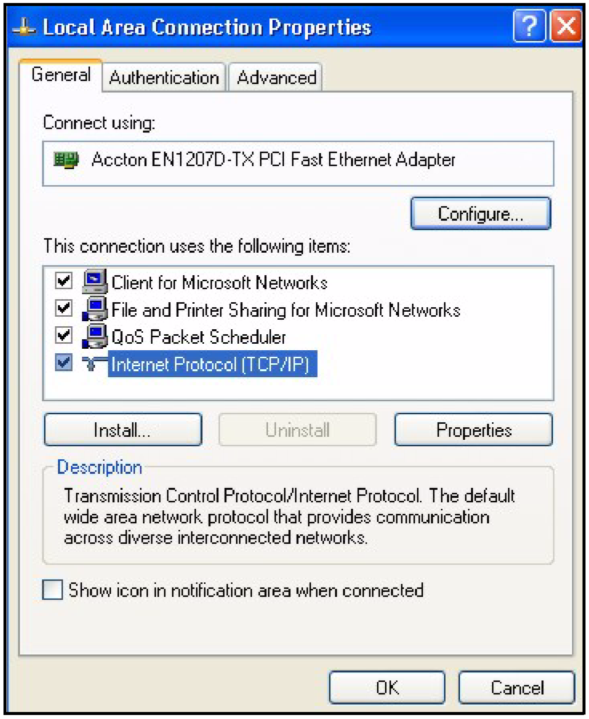
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 121 Windows XP: Control Panel: Network Connections: Properties



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

Figure 122 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

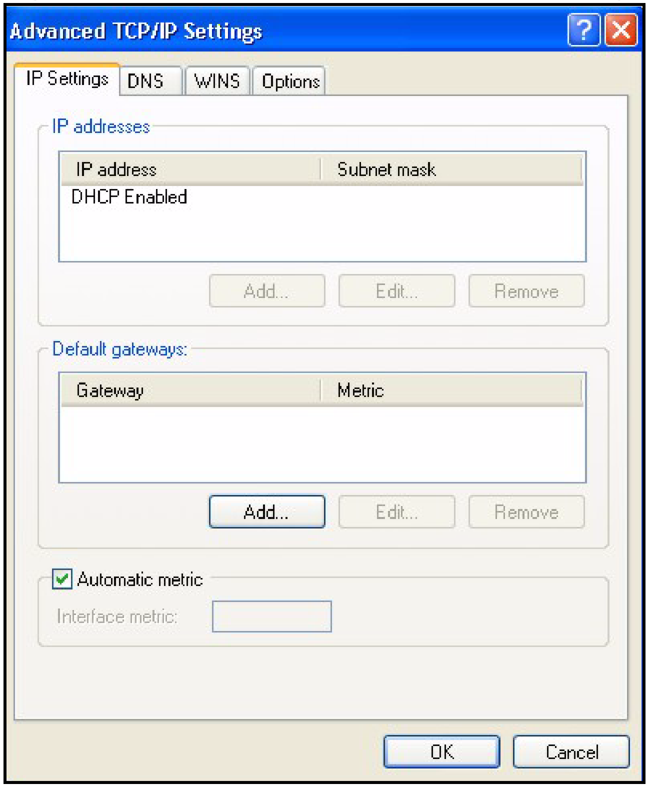
☐ Show icon in notification area when connected

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 123 Windows XP: Advanced TCP/IP Settings



IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

Gateway	Metric

☑ Automatic metric

Interface metric:

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

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

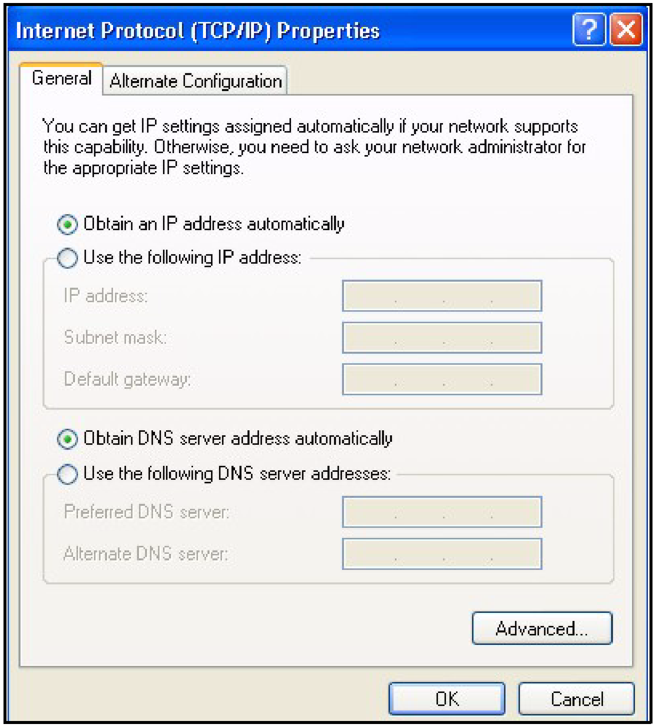
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP 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 124 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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

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

10Turn on your ZyAIR and restart your computer (if prompted).

Verifying Settings

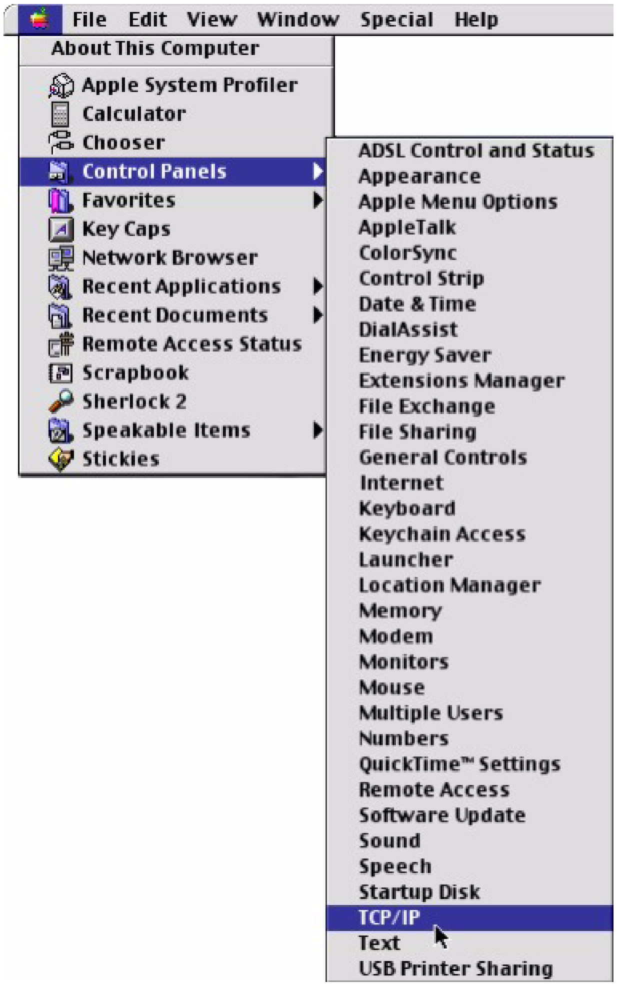
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

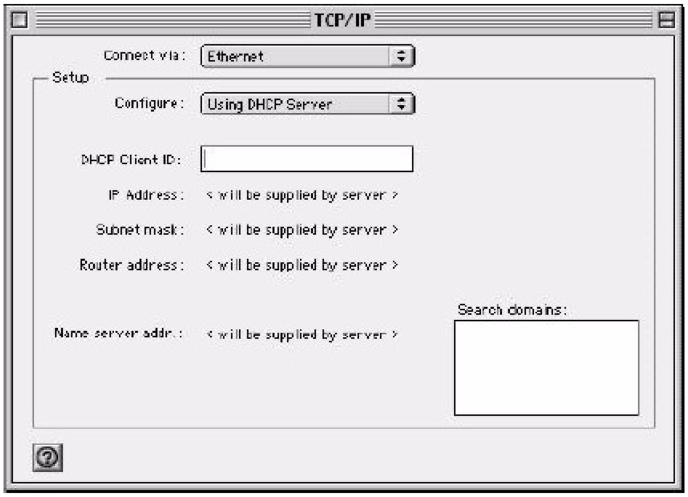
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 125 Macintosh OS 8/9: Apple Menu



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

Figure 126 Macintosh OS 8/9: TCP/IP



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

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).

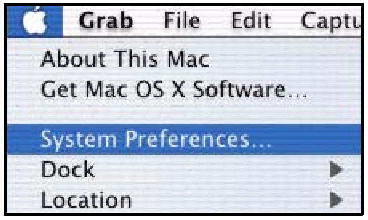
Verifying Settings

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 127 Macintosh OS X: Apple Menu

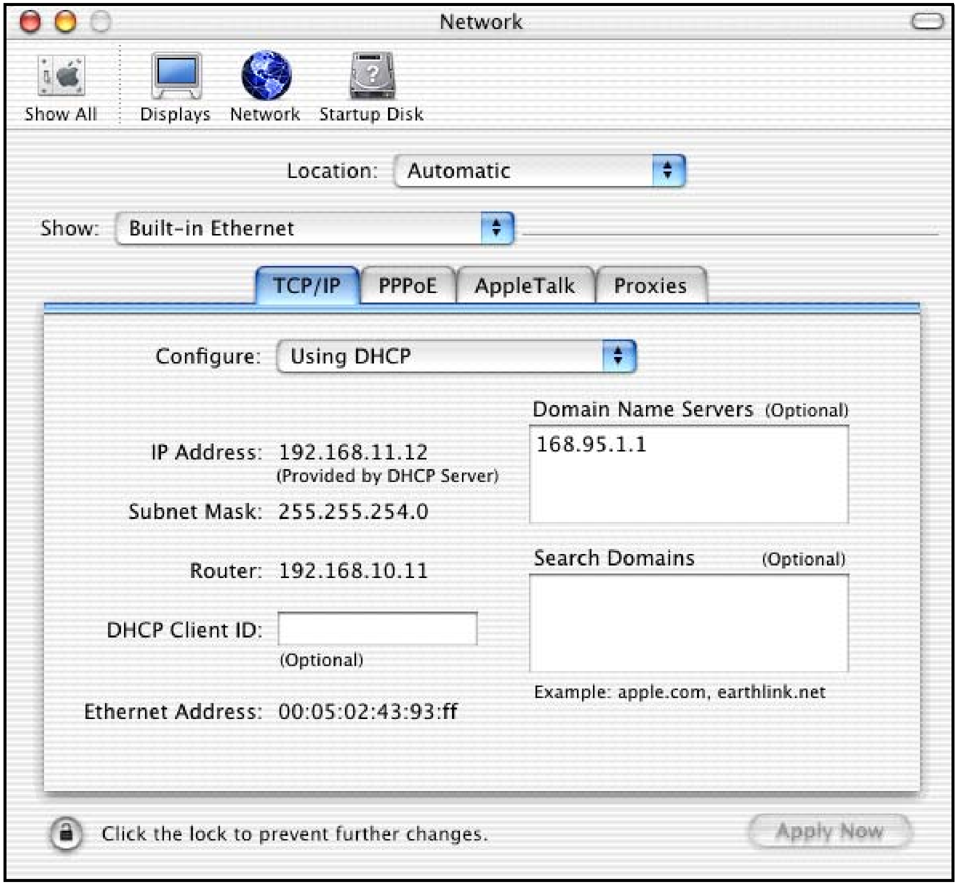


2 Click **Network** in the icon bar.

- 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 128 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

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.

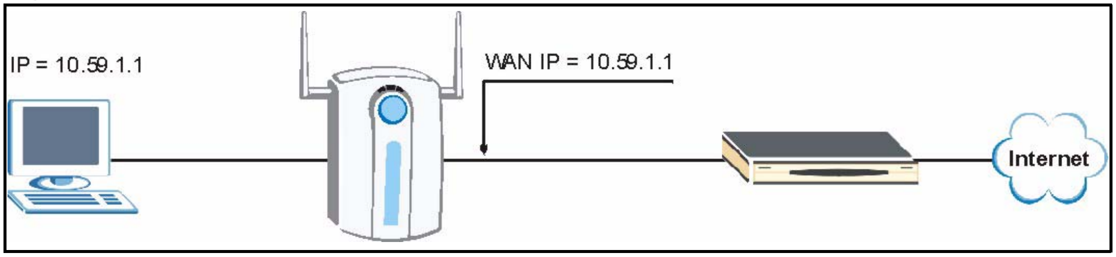
Appendix F
IP Address Assignment Conflicts

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 129 IP Address Conflicts: CaseA

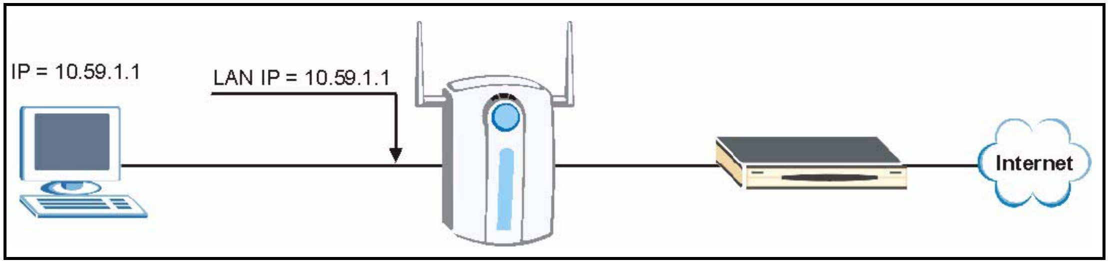


You must set the ZyAIR to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyAIR. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyAIR use a public WAN IP address.

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 130 IP Address Conflicts: Case B

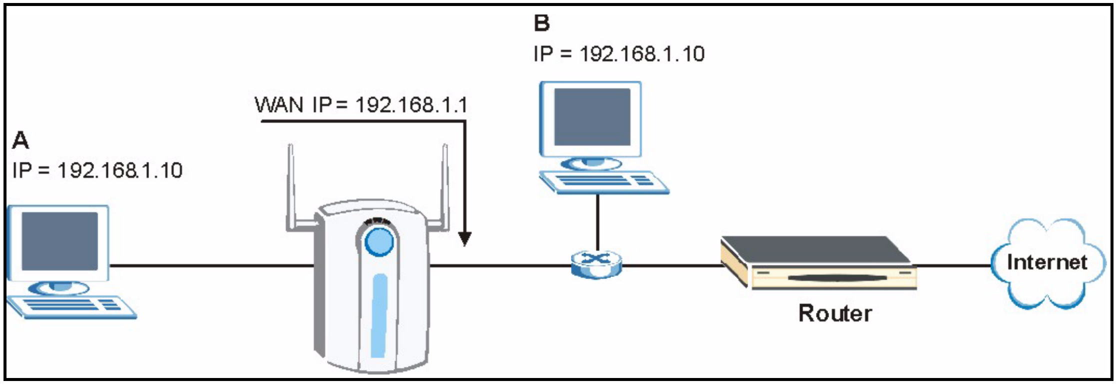


To solve this problem, make sure the ZyAIR LAN IP address is not in the DHCP IP address pool.

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 131 IP Address Conflicts: Case C



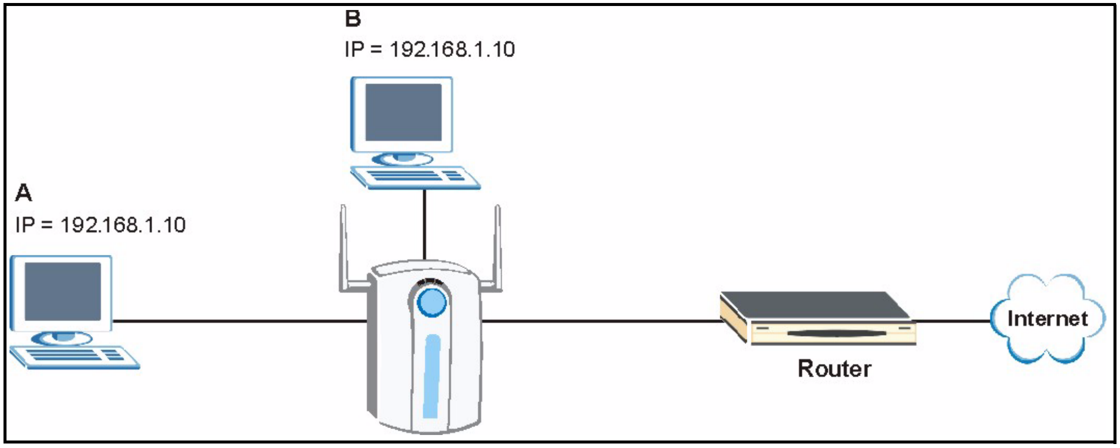
You must set the ZyAIR to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyAIR. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyAIR use a public WAN IP address.

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 132 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

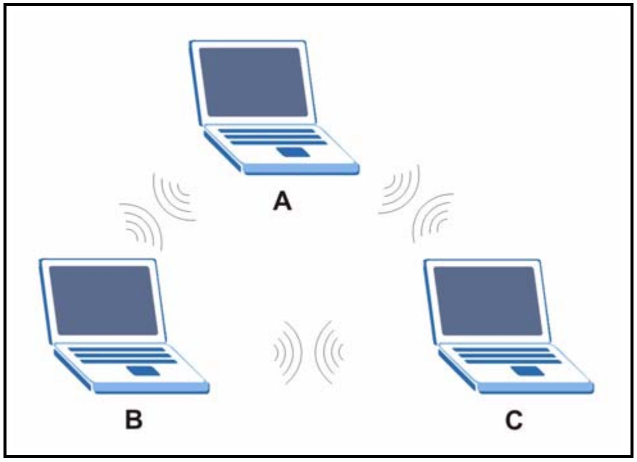
Wireless LAN Topologies

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 133 Peer-to-Peer Communication in an Ad-hoc Network

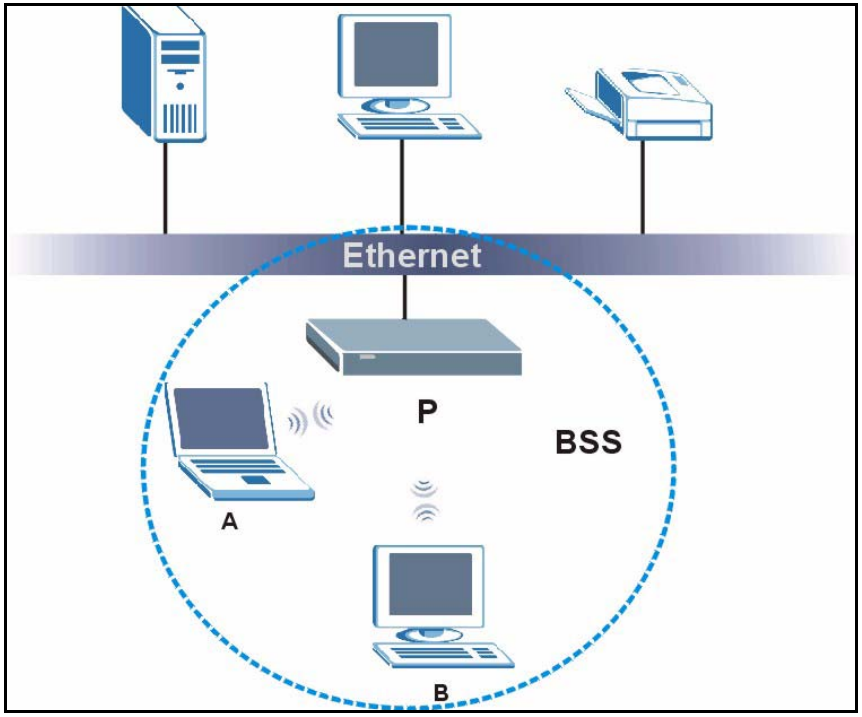


BSS

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 134 Basic Service Set



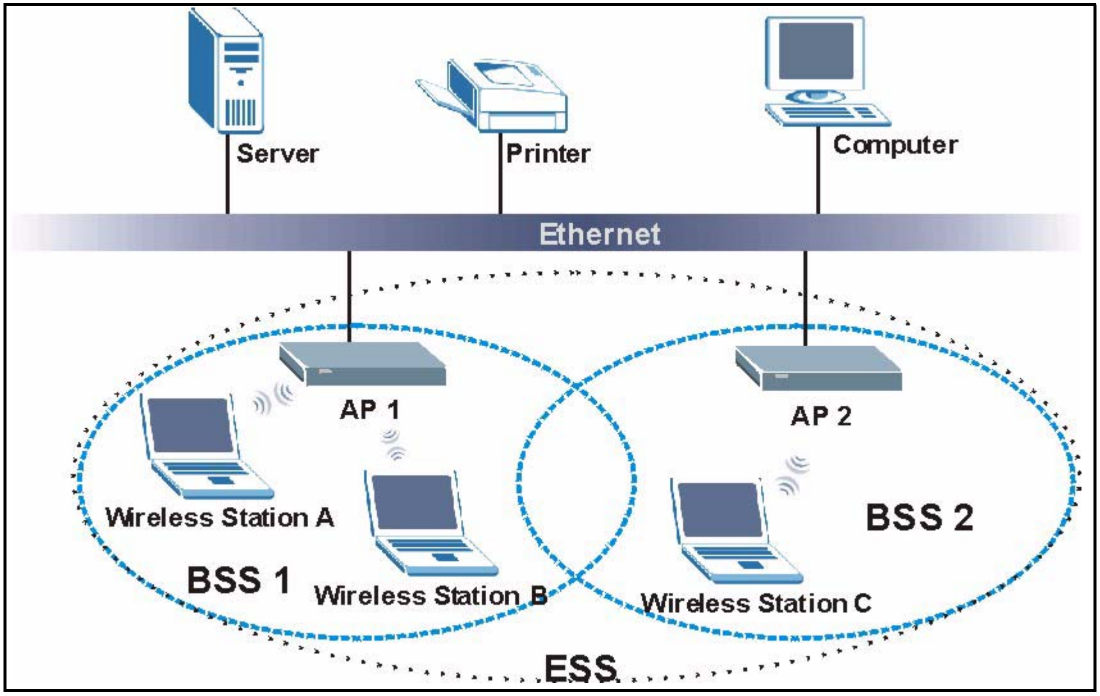
ESS

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 135 Infrastructure WLAN



Channel

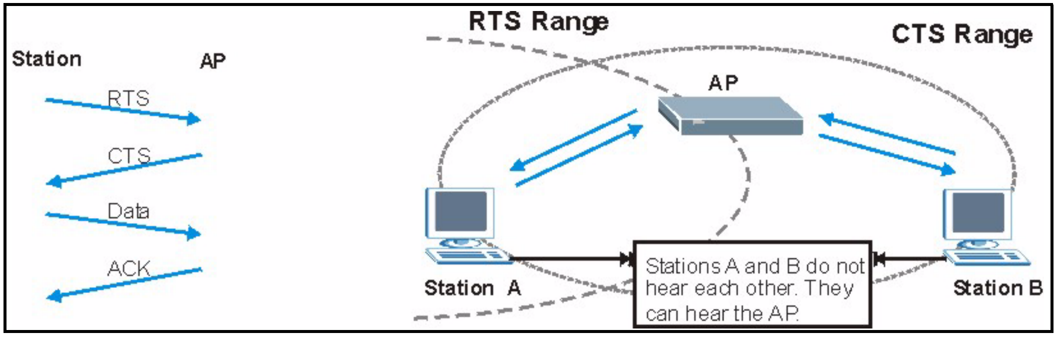
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs 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 136 RTS/CTS


RTS Range
CTS Range
Station
AP
RTS
CTS
Data
ACK
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP.

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 68 IEEE 802.11b

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shifted Keying)
2	DQPSK (Differential Quadrature Phase Shifted Keying)
	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 69 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

User Authentication

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

Encryption

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

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

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

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

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

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

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

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

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 70 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
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 71 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

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 72 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	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 73 “Natural” Masks

	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 74 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 75 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.

Table 76 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
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 77 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
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.**11**000000) 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 78 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 79 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 80 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 81 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 82 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 83 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 71) available for subnetting.

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

Table 84 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 85 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 86 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 86 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 87 Sys log

LOG MESSAGE	DESCRIPTION
`Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>"`	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 88 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 89 North American Plug Standards

AC Power Adaptor Model	AD48-1201200DUY
Input Power	AC120Volts/60Hz/0.25A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1950, CSA C22.2 No.234-M90)

Table 90 North American Plug Standards

AC Power Adaptor Model	DV-121A2-5720
Input Power	AC120Volts/60Hz/27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223-M91)

Table 91 European Plug Standards

AC Power Adaptor Model	AD-1201200DV
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950)

Table 92 United Kingdom Plug Standards

AC Power Adaptor Model	AD-1201200DK
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950, BS7002)

Table 93 Japan Plug Standards

AC Power Adaptor Model	JOD-48-1124
Input Power	AC100Volts/ 50/60Hz/ 27VA
Output Power	DC12Volts/1.2A

Table 93 Japan Plug Standards

Power Consumption	10 W
Safety Standards	T-Mark (Japan Dentori)

Table 94 Australia and New Zealand Plug Standards

AC Power Adaptor Model	AD-1201200DS or AD-121200DS
Input Power	AC240Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	NATA (AS 3260)

Index

Numerics

110V AC **5**
230V AC **5**

A

Abnormal Working Conditions **6**
AC **5**
Accessories **5**
Acts of God **6**
Address Assignment **47**, **94**
Airflow **5**
Alternative Subnet Mask Notation **200**
Antenna
  Directional **213**
  Omni-directional **213**
Antenna gain **212**
AP (access point) **190**
Applications **30**
Authentication databases **79**
Authority **3**
Auto-crossover Ethernet/Fast Ethernet Interface **26**
Auto-negotiating Ethernet/Fast Ethernet Interface **26**
auto-negotiation **26**

B

Backup **106**
backup **145**
Basement **5**
Brute-Force Password Guessing Protection **29**
BSS **188**

C

CA **195**
Cables, Connecting **5**
Certificate Authority **195**
Certifications **3**
Changes or Modifications **3**
Channel **44**, **190**
  Interference **190**
Channel ID **60**, **120**
Charge **6**
Circuit **3**
Class B **3**
Collision **139**
Command Interpreter **156**
Communications **3**
Community **129**
Compliance, FCC **3**
Components **6**
Condition **6**
Connecting Cables **5**
Consequential Damages **6**
Contact Information **7**
Contacting Customer Support **7**
Copyright **2**
Correcting Interference **3**
Corrosive Liquids **5**
Covers **5**
CPU Load **139**
CTS (Clear to Send) **191**
Customer Support **7**

D

Damage **5**
Dampness **5**
Danger **5**
Data encryption **44**
Dealer **3**

Default **107**
Defective **6**
Denmark, Contact Information **7**
DHCP **141**
Diagnostic **142**
Diagnostic Tools **138**
Disclaimer **2**
Discretion **6**
Distribution System (DS) **75**
Dust **5**
Dynamic WEP Key Exchange **195**

E

EAP **29**, **56**
EAP Authentication **194**
Electric Shock **5**
Electrocution **5**
Encryption **196**
Equal Value **6**
Error Log **141**
Error/Information Messages
    Sample **142**
ESS **189**
ESS ID **44**
Europe **5**
Exposure **5**
Extended Service Set **189**
Extended Service Set IDentification **59**

F

Failure **6**
FCC **3**
    Compliance **3**
    Rules, Part 15 **3**
FCC Rules **3**
Federal Communications Commission **3**
Filename Conventions **144**
Finland, Contact Information **7**
Firmware File
    Maintenance **104**
Fitness **6**
Fragment Threshold **120**
Fragmentation Threshold **191**
Fragmentation threshold **191**
France, Contact Information **7**
FTP File Transfer **151**
Functionally Equivalent **6**

G

General Setup **45**, **50**, **116**
General Specifications **168**
Germany, Contact Information **7**
God, act of **6**

H

Harmful Interference **3**
Hidden Menus **112**
Hidden node **190**
High Voltage Points **5**
Host **51**
Host IDs **198**
HyperTerminal program **149**

I

IBSS **188**
IEEE 802.1x **29**
Independent Basic Service Set **103**, **188**
Indirect Damages **6**
initialization vector (IV) **196**
Insurance **6**
Interference **3**
Interference Correction Measures **3**
Interference Statement **3**
Internet access **118**
Internet Security Gateway **26**
IP Address **47**, **94**, **95**, **119**, **141**, **143**
IP Addressing **198**
IP Classes **198**

L

Labor **6**
Legal Rights **6**
Liability **2**

License 2
Lightning 5
Link type 139
Liquids, Corrosive 5
Log and Trace 142
Log Descriptions 208
Logs 96

M

MAC address 73
MAC Address Filter Action 74, 123
MAC Address Filtering 121
MAC Filter 73
MAC filter 57
MAC Filtering 29
MAC service data unit 60
Main Menu 113
Management Information Base (MIB) 129
Materials 6
Merchantability 6
Message Integrity Check (MIC) 196
Modifications 3
MSDU 60

N

Network Management 30
New 6
North America 5
North America Contact Information 7
Norway, Contact Information 7

O

Opening 5
Operating Condition 6
Out-dated Warranty 6
Outlet 3

P

Packets 139
Pairwise Master Key (PMK) 196
Parts 6
Password 51, 110, 129
Patent 2
Permission 2
Photocopying 2
Ping 143
PoE 27
Pool 5
Postage Prepaid. 6
Power Adaptor 5
Power Cord 5
Power Outlet 5
Power over Ethernet 27
Power Specification 168
Power Supply 5
Power Supply, repair 5
Preamble Mode 192
Pre-Shared Key
  Format 75
Private IP Address 47, 94
Product Model 7
Product Page 4
Product Serial Number 7
Products 6
Proof of Purchase 6
Proper Operating Condition 6
Purchase, Proof of 6
Purchaser 6

Q

Qualified Service Personnel 5
Quick Start Guide 40

R

Radio Communications 3
Radio Frequency Energy 3
Radio Interference 3
Radio Reception 3
Radio Technician 3
RADIUS 29, 193

Shared Secret Key **194**
RADIUS Message Types **193**
RADIUS Messages **193**
RAS **140**
Rate
Receiving **139**
Transmission **139**
ReAuthentication Time **78**
Receiving Antenna **3**
Registered **2**
Registered Trademark **2**
Regular Mail **7**
Related Documentation **24**
Relocate **3**
Re-manufactured **6**
Remote Authentication Dial In User Service **29**
Remote Node **139**
Removing **5**
Reorient **3**
Repair **5**, **6**
Replace **6**
Replacement **6**
Reproduction **2**
Required fields **113**
Reset Button **26**
Restore **6**, **106**
Restore Configuration **149**
Return Material Authorization (RMA) Number **6**
Returned Products **6**
Returns **6**
Rights **2**
Rights, Legal **6**
Risk **5**
Risks **5**
RMA **6**
Roaming **65**
Requirements **67**
RTS (Request To Send) **191**
RTS Threshold **120**, **190**, **191**
RTS/CTS handshake **60**

S

Safety Warnings **5**
Security Parameters **197**
Separation Between Equipment and Receiver **3**
Serial Number **7**
Service **5**, **6**
Service Personnel **5**
Service Set **59**
Shipping **6**
Shock, Electric **5**
SMT Menu Overview **111**
SNMP **30**
Community **130**
Configuration **129**
Get **129**
GetNext **129**
Manager **128**
MIBs **129**
Set **129**
Trap **129**
Traps **130**
Trusted Host **130**
Spain, Contact Information **7**
SSL Passthrough **29**
STP (Spanning Tree Protocol) **29**
Subnet Mask **47**, **94**, **119**, **141**
Subnet Masks **199**
Subnetting **199**
Supply Voltage **5**
Support E-mail **7**
Sweden, Contact Information **8**
Swimming Pool **5**
Syntax Conventions **25**
System
Console Port Speed **141**
Diagnostic **142**
Log and Trace **141**
System Information **140**
System Status **138**
Time and Date **161**
System Information **139**
System Information & Diagnosis **138**
System Maintenance **138**, **140**, **145**, **147**, **149**, **150**, **153**, **154**, **156**, **162**
System Name **50**

T

Tampering **6**
TCP/IP **143**
Telephone **7**
Television Interference **3**
Television Reception **3**
Temporal Key Integrity Protocol (TKIP) **196**
TFTP File Transfer **152**
Thunderstorm **5**

Time and Date Setting **162**
Time Setting **52**
Time Zone **163**
Trace Records **141**
Trademark **2**
Trademark Owners **2**
Trademarks **2**
Translation **2**
Troubleshooting
  Accessing ZyAIR **165**
  Ethernet Port **164**
  Start-Up **164**
TV Technician **3**

U

Undesired Operations **3**
Upload Firmware **150**
User Authentication **196**
User Profiles **126**

V

Valid CI Commands **157**
Value **6**
Vendor **5**
Ventilation Slots **5**
Viewing Certifications **3**, **4**
VLAN **28**
Voltage Supply **5**
Voltage, High **5**

W

Warnings **5**
Warranty **6**
Warranty Information **7**
Warranty Period **6**
Water **5**
Web Configurator **40**, **42**
Web Site **7**
WEP **44**
WEP Encryption **29**, **60**, **120**
WEP encryption **58**
Wet Basement **5**
Wi-Fi Protected Access **28**, **75**
Wireless Client WPA Supplicants **76**
Wireless LAN **119**
  Configuring **58**
Wireless LAN Setup **119**
Wireless security **56**
Wizard Setup **44**, **45**, **47**
WLAN
  Interference **190**
  Security parameters **197**
Workmanship **6**
Worldwide Contact Information **7**
WPA **28**, **75**
  Supplicants **76**
  with RADIUS Application Example **75**
WPA -Pre-Shared Key **75**
WPA with RADIUS Application **75**
WPA-PSK **75**
WPA-PSK Application **75**
Written Permission **2**

Z

ZyAIR LED **27**
ZyNOS **2**, **145**
ZyNOS F/W Version **145**
ZyXEL Communications Corporation **2**
ZyXEL Home Page **4**
ZyXEL Limited Warranty
  Note **6**
ZyXEL Network Operating System **2**