

ZyAIR

Access Point Series

User's Guide

Version 3.50

September 2003



Copyright

Copyright © 2003 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

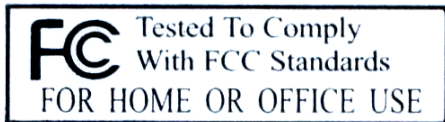
1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Certifications

Refer to the product page at www.zyxel.com.



ZyXEL Limited Warranty

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

Note

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

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

Safety Warnings

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

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 LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science- Based Industrial Park, Hsinchu 300, Taiwan.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0858	www.us.zyxel.com ftp.zyxel.com	
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

Table of Contents

Copyright.....	ii
Federal Communications Commission (FCC) Interference Statement.....	iii
ZyXEL Limited Warranty	iv
Customer Support.....	v
List of Figures	xi
List of Tables	xv
Preface	xvii
OVERVIEW.....	I
Chapter 1 Getting to Know Your ZyAIR.....	1-1
1.1 Introducing the ZyAIR Access Point Series	1-1
1.2 ZyAIR Features.....	1-1
1.3 Applications for the ZyAIR	1-6
1.3.1 Internet Access Application	1-6
1.3.2 Corporation Network Application.....	1-7
Chapter 2 Introducing the Web Configurator	2-1
2.1 Accessing the ZyAIR Web Configurator	2-1
2.2 Resetting the ZyAIR	2-2
2.2.1 Method of Restoring Factory-Defaults	2-2
2.3 Navigating the ZyAIR Web Configurator.....	2-3
Chapter 3 Wizard Setup.....	3-1
3.1 Wizard Setup Overview	3-1
3.1.1 Channel	3-1
3.1.2 ESS ID	3-1
3.1.3 WEP Encryption	3-1
3.2 Wizard Setup: General Setup	3-2
3.3 Wizard Setup: Wireless LAN	3-3
3.4 Wizard Setup: IP Address	3-5
3.4.1 IP Address Assignment	3-5
3.4.2 IP Address and Subnet Mask	3-6
3.5 Basic Setup Complete	3-8
SYSTEM, WIRELESS, VLAN AND IP.....	II
Chapter 4 System Screens.....	4-1
4.1 System Overview	4-1
4.2 Configuring General Setup	4-1
4.3 Configuring Password.....	4-2
4.4 Configuring Time Setting	4-3
Chapter 5 Wireless Configuration and Roaming.....	5-1
5.1 Wireless LAN Overview.....	5-1
5.1.1 IBSS	5-1

5.1.2	BSS.....	5-1
5.1.3	ESS.....	5-2
5.2	Wireless LAN Basics	5-3
5.2.1	RTS/CTS.....	5-3
5.2.2	Fragmentation Threshold	5-4
5.3	Configuring Wireless	5-5
5.4	Configuring Bridge	5-7
5.5	Configuring Roaming.....	5-10
5.5.1	Requirements for Roaming	5-11
Chapter 6	Wireless Security	6-1
6.1	Wireless Security Overview.....	6-1
6.2	WEP Overview.....	6-1
6.2.1	Data Encryption	6-1
6.2.2	Authentication	6-2
6.3	Configuring WEP Encryption	6-3
6.4	MAC Filter.....	6-5
6.5	802.1x Overview	6-7
6.6	Introduction to RADIUS	6-7
6.6.1	EAP Authentication Overview	6-8
6.7	Dynamic WEP Key Exchange	6-9
6.8	Introduction to Local User Database.....	6-10
6.9	Configuring 802.1x	6-10
6.10	Configuring Local User Database	6-13
6.11	Configuring RADIUS	6-14
Chapter 7	Multiple ESS and VLAN	7-1
7.1	Wireless LAN Infrastructures	7-1
7.1.1	Multiple ESS	7-1
7.1.2	Notes on Multiple-ESS.....	7-1
7.1.3	Multiple ESS Example	7-1
7.2	VLAN.....	7-2
7.2.1	Management VLAN ID.....	7-2
7.2.2	Multi-ESS with VLAN Example	7-3
7.3	Configuring Multiple ESS.....	7-3
7.3.1	Edit ESS	7-5
7.3.2	MAC Filter Summary.....	7-7
7.4	Configuring VLAN	7-8
Chapter 8	IP Screen	8-1
8.1	Factory Ethernet Defaults.....	8-1
8.2	TCP/IP Parameters.....	8-1
8.2.1	IP Address and Subnet Mask.....	8-1
8.2.2	WAN IP Address Assignment.....	8-1

8.3	Configuring IP	8-2
LOGS		III
Chapter 9 Logs Screens		9-1
9.1	Configuring View Log	9-1
9.2	Configuring Log Settings	9-2
MAINTENANCE		IV
Chapter 10 Maintenance		10-1
10.1	Maintenance Overview	10-1
10.2	System Status Screen	10-1
10.2.1	System Statistics	10-2
10.3	Wireless Screen	10-3
10.3.1	Association List	10-3
10.3.2	Channel Usage	10-4
10.4	F/W Upload Screen	10-7
10.5	Configuration Screen	10-9
10.5.1	Backup Configuration	10-9
10.5.2	Restore Configuration	10-10
10.5.3	Back to Factory Defaults	10-12
SMT CONFIGURATION		V
Chapter 11 Introducing the SMT		11-1
11.1	Connect to your ZyAIR Using Telnet	11-1
11.2	Changing the System Password	11-1
11.3	ZyAIR SMT Menu Overview Example	11-2
11.4	Navigating the SMT Interface	11-4
11.4.1	System Management Terminal Interface Summary	11-5
Chapter 12 General Setup		12-1
12.1	General Setup	12-1
12.1.1	Procedure To Configure Menu 1	12-1
Chapter 13 LAN Setup		13-1
13.1	LAN Setup	13-1
13.2	TCP/IP Ethernet Setup	13-1
13.3	Wireless LAN Setup	13-2
13.3.1	Configuring MAC Address Filter	13-5
13.3.2	Configuring Roaming	13-7
13.3.3	Configuring Multiple ESS (for ZyAIR B-3000 only)	13-8
13.3.4	Configuring Bridge Link (for ZyAIR B-3000 only)	13-11
Chapter 14 Dial-in User Setup		14-1
14.1	Dial-in User Setup	14-1
Chapter 15 VLAN Setup		15-1
15.1	VLAN Setup	15-1
Chapter 16 SNMP Configuration		16-1

16.1	About SNMP.....	16-1
16.2	Supported MIBs	16-2
16.3	SNMP Configuration	16-2
16.4	SNMP Traps.....	16-3
Chapter 17	System Security	17-1
17.1	System Security.....	17-1
17.1.1	System Password.....	17-1
17.1.2	Configuring External RADIUS Server.....	17-1
17.1.3	802.1x.....	17-3
Chapter 18	System Information and Diagnosis.....	18-1
18.1	System Status	18-1
18.2	System Information	18-3
18.2.1	System Information	18-3
18.2.2	Console Port Speed	18-4
18.3	Log and Trace	18-5
18.3.1	Viewing Error Log	18-5
18.4	Diagnostic	18-5
Chapter 19	Firmware and Configuration File Maintenance.....	19-1
19.1	Filename Conventions.....	19-1
19.2	Backup Configuration	19-2
19.2.1	Backup Configuration Using FTP.....	19-2
19.2.2	Using the FTP command from the DOS Prompt.....	19-3
19.2.3	Backup Configuration Using TFTP	19-4
19.2.4	Example: TFTP Command.....	19-4
19.3	Restore Configuration	19-5
19.4	Uploading Firmware and Configuration Files.....	19-6
19.4.1	Firmware Upload	19-7
19.4.2	Configuration File Upload	19-7
19.4.3	Using the FTP command from the DOS Prompt Example.....	19-8
19.4.4	TFTP File Upload	19-9
19.4.5	Example: TFTP Command.....	19-10
Chapter 20	System Maintenance and Information	20-1
20.1	Command Interpreter Mode	20-1
20.2	Time and Date Setting.....	20-2
20.2.1	Resetting the Time	20-3
APPENDICES	VI	
Appendix A	Troubleshooting.....	A-1
Appendix B	Brute-Force Password Guessing Protection	B-1
Appendix C	Setting up Your Computer's IP Address.....	C-1
Appendix D	Wireless LAN and IEEE 802.11.....	D-1
Appendix E	Wireless LAN With IEEE 802.1x.....	E-1

Appendix F Types of EAP Authentication F-1
Appendix G Power over Ethernet Specifications G-1
Appendix H Antenna Selection and Positioning Recommendation H-1
Appendix I PPPoE I-1
Appendix J PPTP..... J-1
Appendix K IP Subnetting K-1
Appendix L Command Interpreter L-1
Appendix M NetBIOS Filter Commands..... M-1
Appendix N Log Descriptions N-1
Appendix O Power Adaptor Specifications O-1
Appendix P Index..... P-1

List of Figures

Figure 1-1 PoE Installation Example	1-3
Figure 1-2 WDS Functionality Example	1-5
Figure 1-3 Internet Access Application	1-7
Figure 1-4 Corporation Network Application	1-7
Figure 2-1 Change Password Screen	2-1
Figure 2-2 The MAIN MENU Screen of the Web Configurator	2-3
Figure 3-1 Wizard 1 : General Setup	3-2
Figure 3-2 Wizard 2 : Wireless LAN Setup	3-4
Figure 3-3 Wizard 3 : IP Address Assignment	3-7
Figure 4-1 System General Setup	4-1
Figure 4-2 Password	4-3
Figure 4-3 Time Setting	4-4
Figure 5-1 IBSS (Ad-hoc) Wireless LAN	5-1
Figure 5-2 Basic Service set	5-2
Figure 5-3 Extended Service Set	5-3
Figure 5-4 RTS/CTS	5-4
Figure 5-5 Wireless	5-5
Figure 5-6 Bridging Example	5-7
Figure 5-7 Bridge Loop: Two Bridges Connected to Hub	5-7
Figure 5-8 Bridge Loop: Bridge Connected to Wired LAN	5-8
Figure 5-9 Wireless : Bridge	5-9
Figure 5-10 Roaming Example	5-10
Figure 5-11 Roaming	5-11
Figure 6-1 ZyAIR Wireless Security Levels	6-1
Figure 6-2 WEP Authentication Steps	6-2
Figure 6-3 Wireless	6-3
Figure 6-4 MAC Address Filter	6-6
Figure 6-5 EAP Authentication	6-9
Figure 6-6 802.1x Authentication	6-10
Figure 6-7 Local User Database	6-13
Figure 6-8 RADIUS	6-14
Figure 7-1 Multi-ESS Example	7-2
Figure 7-2 Multi-ESS with VLAN Example	7-3
Figure 7-3 Wireless : Multiple ESS	7-4
Figure 7-4 Wireless : Edit ESS	7-6
Figure 7-5 MAC Filter Summary	7-8
Figure 7-6 VLAN	7-9
Figure 8-1 IP Setup	8-2
Figure 9-1 View Log	9-1

Figure 9-2 Log Settings	9-3
Figure 10-1 System Status	10-1
Figure 10-2 System Status: Show Statistics.....	10-2
Figure 10-3 Association List.....	10-4
Figure 10-4 Channel Usage (ZyAIR B-1000).....	10-5
Figure 10-5 Channel Usage	10-6
Figure 10-6 Firmware Upload	10-7
Figure 10-7 Firmware Upload In Process.....	10-8
Figure 10-8 Network Temporarily Disconnected.....	10-8
Figure 10-9 Firmware Upload Error	10-9
Figure 10-10 Backup Configuration	10-10
Figure 10-11 Restore Configuration	10-10
Figure 10-12 Configuration Upload Successful.....	10-11
Figure 10-13 Network Temporarily Disconnected.....	10-11
Figure 10-14 Configuration Upload Error	10-12
Figure 10-15 Back to Factory Default	10-12
Figure 10-16 Reset Warning Message	10-13
Figure 11-1 Login Screen	11-1
Figure 11-2 Menu 23.1 System Security : Change Password	11-2
Figure 11-3 ZyAIR B-3000 SMT Menu Overview Example	11-3
Figure 11-4 ZyAIR B-3000 SMT Main Menu.....	11-5
Figure 12-1 Menu 1 General Setup.....	12-1
Figure 13-1 Menu 3 LAN Setup	13-1
Figure 13-2 Menu 3.2 TCP/IP Setup.....	13-1
Figure 13-3 Menu 3.5 Wireless LAN Setup	13-3
Figure 13-4 Menu 3.5 Wireless LAN Setup	13-5
Figure 13-5 Menu 3.5.1 WLAN MAC Address Filter	13-6
Figure 13-6 Menu 3.5 Wireless LAN Setup	13-7
Figure 13-7 Menu 3.5.2 Roaming Configuration	13-7
Figure 13-8 Menu 3.5 Wireless LAN Setup	13-8
Figure 13-9 Menu 3.5.3 Multiple ESS Configuration.....	13-9
Figure 13-10 Menu 3.5.3.1 ESS x Configuration	13-10
Figure 13-11 Menu 3.5 Wireless LAN Setup.....	13-11
Figure 13-12 Menu 3.5.4 Bridge Link Configuration.....	13-12
Figure 14-1 Menu 14- Dial-in User Setup	14-1
Figure 14-2 Menu 14.1- Edit Dial-in User.....	14-1
Figure 15-1 Menu 16 VLAN Setup	15-1
Figure 16-1 SNMP Management Model.....	16-1
Figure 16-2 Menu 22 SNMP Configuration	16-3
Figure 17-1 Menu 23 System Security	17-1
Figure 17-2 Menu 23 System Security	17-1

Figure 17-3 Menu 23.2 System Security : RADIUS Server	17-2
Figure 17-4 Menu 23 System Security.....	17-3
Figure 17-5 Menu 23.4 System Security : IEEE802.1x	17-4
Figure 18-1 Menu 24 System Maintenance	18-1
Figure 18-2 Menu 24.1 System Maintenance : Status.....	18-2
Figure 18-3 Menu 24.2 System Information and Console Port Speed	18-3
Figure 18-4 Menu 24.2.1 System Information : Information	18-3
Figure 18-5 Menu 24.2.2 System Maintenance : Change Console Port Speed	18-4
Figure 18-6 Menu 24.3 System Maintenance : Log and Trace	18-5
Figure 18-7 Sample Error and Information Messages	18-5
Figure 18-8 Menu 24.4 System Maintenance : Diagnostic	18-6
Figure 19-1 Menu 24.5 Backup Configuration	19-2
Figure 19-2 FTP Session Example	19-3
Figure 19-3 Menu 24.6 Restore Configuration	19-6
Figure 19-4 Menu 24.7 System Maintenance : Upload Firmware	19-6
Figure 19-5 Menu 24.7.1 System Maintenance : Upload System Firmware.....	19-7
Figure 19-6 Menu 24.7.2 System Maintenance : Upload System Configuration File.....	19-8
Figure 19-7 FTP Session Example	19-9
Figure 20-1 Menu 24 System Maintenance	20-1
Figure 20-2 Valid CI Commands	20-1
Figure 20-3 Menu 24.10 System Maintenance : Time and Date Setting.....	20-2

List of Tables

Table 1-1 Model Specific Features.....	1-1
Table 3-1 Wizard 1 : General Setup	3-3
Table 3-2 Wizard 2 : Wireless LAN Setup	3-4
Table 3-3 Private IP Address Ranges	3-5
Table 3-4 Wizard 3 : IP Address Assignment	3-7
Table 4-1 System General Setup	4-2
Table 4-2 Password	4-3
Table 4-3 Time Setting	4-4
Table 5-1 Wireless.....	5-6
Table 5-2 Wireless : Bridge.....	5-9
Table 5-3 Roaming.....	5-12
Table 6-1 Wireless.....	6-4
Table 6-2 MAC Address Filter.....	6-6
Table 6-3 802.1x Authentication	6-11
Table 6-4 Local User Database	6-14
Table 6-5 RADIUS.....	6-15
Table 7-1 Wireless : Multiple ESS	7-5
Table 7-2 Wireless : Edit ESS	7-6
Table 7-3 MAC Filter Summary	7-8
Table 7-4 VLAN	7-9
Table 8-1 Private IP Address Ranges	8-1
Table 8-2 IP Setup.....	8-2
Table 9-1 View Log.....	9-2
Table 9-2 Log Settings	9-3
Table 10-1 System Status	10-1
Table 10-2 System Status: Show Statistics.....	10-2
Table 10-3 Association List.....	10-4
Table 10-4 Channel Usage (ZyAIR B-1000)	10-5
Table 10-5 Channel Usage	10-6
Table 10-6 Firmware Upload	10-8
Table 10-7 Restore Configuration	10-11
Table 11-1 Main Menu Commands.....	11-4
Table 11-2 Main Menu Summary	11-5
Table 12-1 Menu 1 General Setup.....	12-2
Table 13-1 Menu 3.2 TCP/IP Setup	13-2
Table 13-2 Menu 3.5 Wireless LAN Setup	13-3
Table 13-3 Menu 3.5.1 WLAN MAC Address Filter	13-6
Table 13-4 Menu 3.5.2 Roaming Configuration	13-8
Table 13-5 Menu 3.5.3 Multiple ESS Configuration	13-9

Table 13-6 Menu 3.5.3.1 ESS x Configuration.....	13-10
Table 13-7 Menu 3.5.4 Bridge Link Configuration	13-12
Table 14-1 Menu 14.1- Edit Dial-in User	14-2
Table 15-1 Menu 16 VLAN Setup.....	15-1
Table 16-1 Menu 22 SNMP Configuration.....	16-3
Table 16-2 SNMP Traps.....	16-4
Table 16-3 Ports and Interface Types.....	16-4
Table 17-1 Menu 23.2 System Security : RADIUS Server.....	17-2
Table 17-2 Menu 23.4 System Security : IEEE802.1x	17-4
Table 18-1 Menu 24.1 System Maintenance : Status.....	18-2
Table 18-2 Menu 24.2.1 System Maintenance : Information.....	18-4
Table 18-3 Menu 24.4 System Maintenance Menu : Diagnostic	18-6
Table 19-1 Filename Conventions	19-2
Table 19-2 General Commands for Third Party FTP Clients.....	19-3
Table 19-3 General Commands for Third Party TFTP Clients	19-5
Table 20-1 Menu 24.10 System Maintenance : Time and Date Setting	20-3

Preface

Congratulations on your purchase from the ZyAIR Access Point (AP) series.

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

Some features are not available in every model. Refer to the *Model Specific Features* table in Chapter 1 of this user's guide to see what features are specific to your ZyAIR model.

This User's Guide is designed to guide you through the configuration of your ZyAIR using the web configurator or the SMT.

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.

The web configurator parts of this guide contain background information on features configurable by the web configurator and the SMT. The SMT parts of this guide contain background information on features not configurable by the web configurator.

Related Documentation

- **Supporting Disk**
Refer to the included CD for support documents.
- **Quick Installation Guide**
Our Quick Installation Guide is designed to help you get up and running right away. It contains information on the configuration of key features and hardware connections and installation.
- **ZyXEL Web Site**
The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

Syntax Conventions

- “Enter” means for you to type one or more characters (and press the carriage return). “Select” or “Choose” means for you to use one predefined choices.
- Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.

- 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 Access Point series may be referred to simply as the ZyAIR in the user's guide.

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.

Part I:

OVERVIEW

This part introduces the main features and applications of ZyAIR and shows how to access the web configurator and use the Wizard to configure for Internet Access.

Chapter 1

Getting to Know Your ZyAIR

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

1.1 Introducing the ZyAIR Access Point Series

The ZyAIR Access Point extends the range of your existing wired network without any additional wiring efforts. The ZyAIR provides easy network access to mobile users. 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 and SNMP network management enables remote configuration and management of your ZyAIR.

1.2 ZyAIR Features

The following sections describe the features of the ZyAIR Access Point series. Features vary by ZyAIR model. This table lists the difference between models; it does not include features that are common to all of the ZyAIR models.

Some features are not available in every model. Refer to the *Model Specific Features* table to see what features are specific to your ZyAIR model. These features are defined at the time of writing.

Table 1-1 Model Specific Features

ZYAIR MODEL	B-1000	B-1000 v.2	B-3000
FEATURES			
Two 2dBi Dipole Antennas	Detachable	Detachable	Detachable
GUI Enable/Disable Capability of ZyAIR WLAN LED ON/OFF		O	O
Multiple-ESSID/VLAN of WLAN			O
Limitation of Client Connections		O	O
Configurable Output Power		O	O
SSL Passthrough	O	O	O

Table 1-1 Model Specific Features

<div>ZYAIR MODEL</div> <div>FEATURES</div>	B-1000	B-1000 v.2	B-3000
Power over Ethernet			O
Bridge/Repeater			O
AP & WDS (Wireless Distribution System) Support Concurrently			O
Table Key: An “O” in a model’s column shows that the model has the specified feature. A number specific to an individual model may alternately be displayed. The information in this table was correct at the time of writing, although it may be subject to change.			

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

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

Reset Button

The ZyAIR reset button is built into the top 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.

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.

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

A Bridge/Repeater link LED turns steady on green when your ZyAIR acts as a bridge, establishing a wireless link to another AP. It turns steady on orange when your ZyAIR acts as a repeater, establishing wireless links to two or more 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.

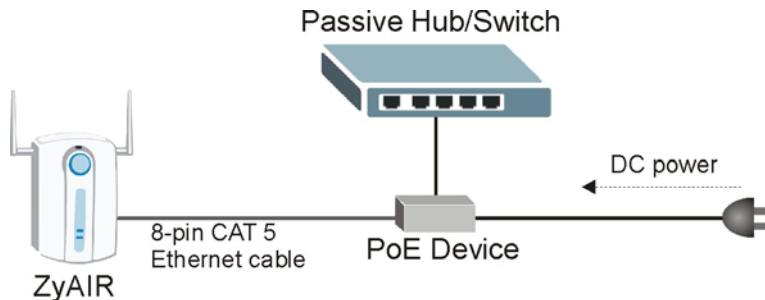


Figure 1-1 PoE Installation Example

802.11b Wireless LAN Standard

ZyAIR products containing the letter “B” in the model name, such as ZyAIR B-1000, ZyAIR B-1020, comply with the 802.11b wireless standard.

The 802.11b data rate and corresponding modulation techniques are as follows. The modulation technique defines how bits are encoded onto radio waves.

802.11b	
Data Rate (Mbps)	Modulation
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)

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.

Output Power Management

Output Power Management is the ability to set the level of output power.

There may be interference or difficulty with channel assignment when there is a high density of APs within a coverage area. In this case you can lower the output power of each access point, thus enabling you to place access points closer together.

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). This feature is not available on all models.

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) with multi-ESS to extend the wireless logical grouping to the wired network. Each ESS is assigned a unique VLAN ID. This feature is not available on all models.

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.

Wireless LAN MAC Address Filtering

Your ZyAIR checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.

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.

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.

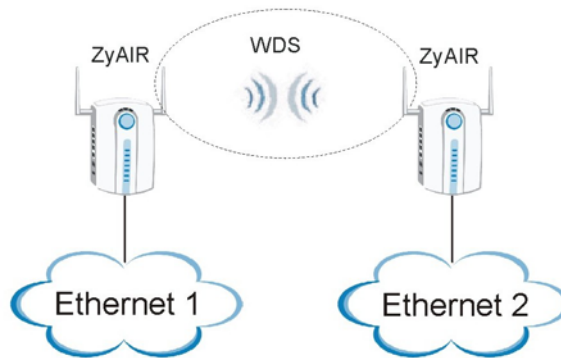


Figure 1-2 WDS Functionality Example

SNMP

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

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyAIR's management settings. Most functions of the ZyAIR are also software configurable via the SMT

(System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator over a telnet connection.

Logging and Tracing

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

Embedded FTP and TFTP Servers

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

Wireless Association List

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

Wireless LAN Channel Usage

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

1.3 Applications for the ZyAIR

Here are some application examples of what you can do with your ZyAIR.

1.3.1 Internet Access Application

The ZyAIR is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyAIR is shown as follows.

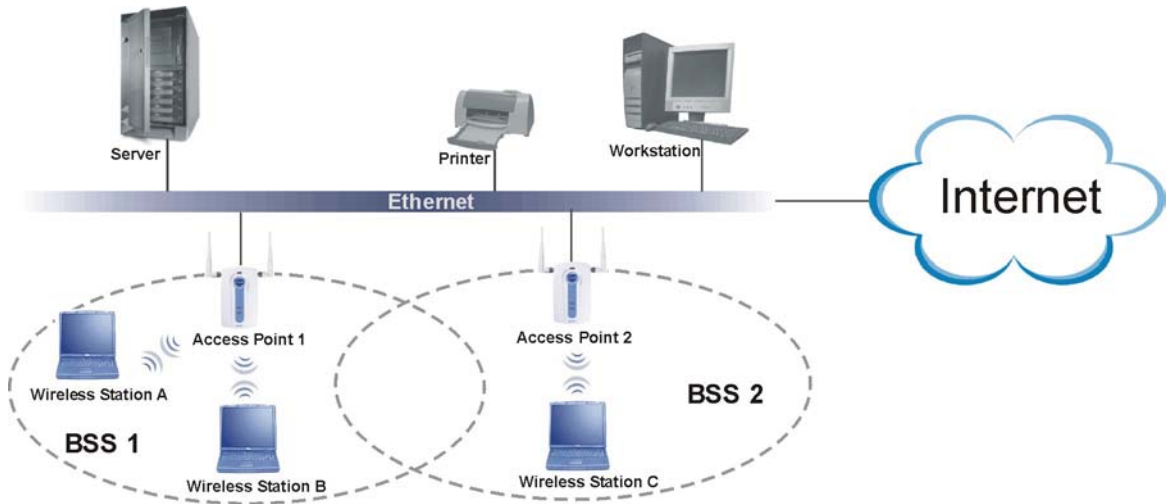


Figure 1-3 Internet Access Application

1.3.2 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. The two computers with wireless adapters are allowed to access the network resource through the ZyAIR after account validation by the network authentication server.

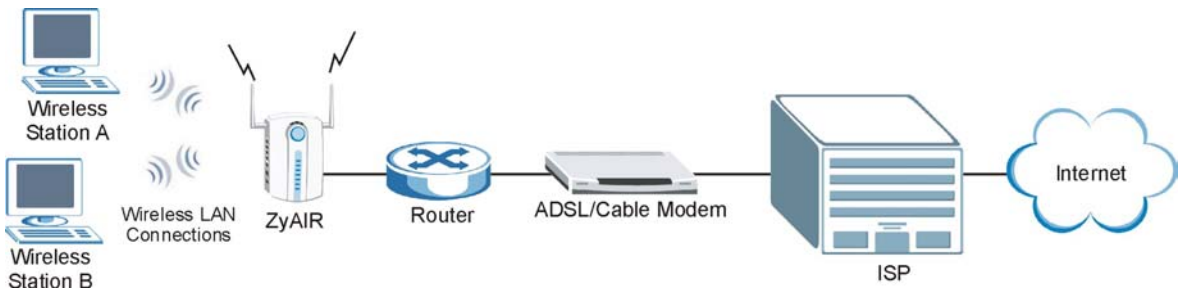


Figure 1-4 Corporation Network Application

Chapter 2

Introducing the Web Configurator

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

2.1 Accessing the ZyAIR Web Configurator

- Step 1.** Make sure your ZyAIR hardware is properly connected (refer to the Quick Installation Guide).
- Step 2.** Prepare your computer/computer network to connect to the ZyAIR (refer to the appendix).
- Step 3.** Launch your web browser.
- Step 4.** Type "192.168.1.2" (default) as the URL.
- Step 5.** Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- Step 6.** 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** to allow access without password change.

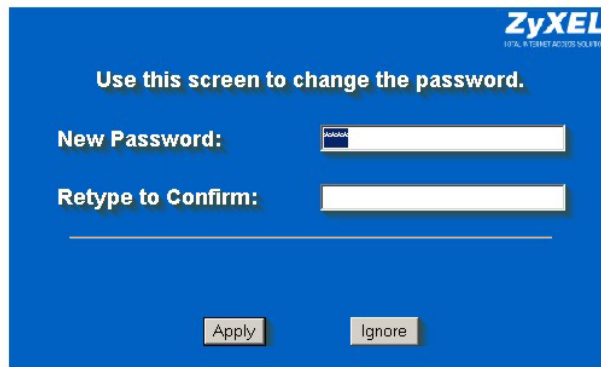
The image shows a web-based password change interface with a blue background. At the top right is the ZyXEL logo with the tagline 'TOTAL WIRELESS ACCESS SOLUTION'. The main heading reads 'Use this screen to change the password.' Below this are two input fields: 'New Password:' and 'Retype to Confirm:'. The 'New Password' field has a small blue icon on its left. At the bottom are two buttons: 'Apply' and 'Ignore'.

Figure 2-1 Change Password Screen

- Step 7.** You should now see the **MAIN MENU** screen.

The ZyAIR automatically times out after five minutes of inactivity. Simply log back into the ZyAIR if this happens to you.

2.2 Resetting the ZyAIR

If you forget your password or cannot access the ZyAIR, you will need to reload the factory-default configuration file or use the **RESET** button on the top 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”, also.

2.2.1 Method of Restoring Factory-Defaults


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

1. Use the **RESET** button on the top panel of the ZyAIR to upload the default configuration file (hold this button in for about 10 seconds or until the Link LED turns red). Use this method for cases when the password or IP address of the ZyAIR is not known.
2. Use the web configurator to restore defaults (refer to the *Maintenance* chapter).
3. Transfer the configuration file to your ZyAIR using FTP. See later in the part on SMT configuration for more information.

2.3 Navigating the ZyAIR Web Configurator

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

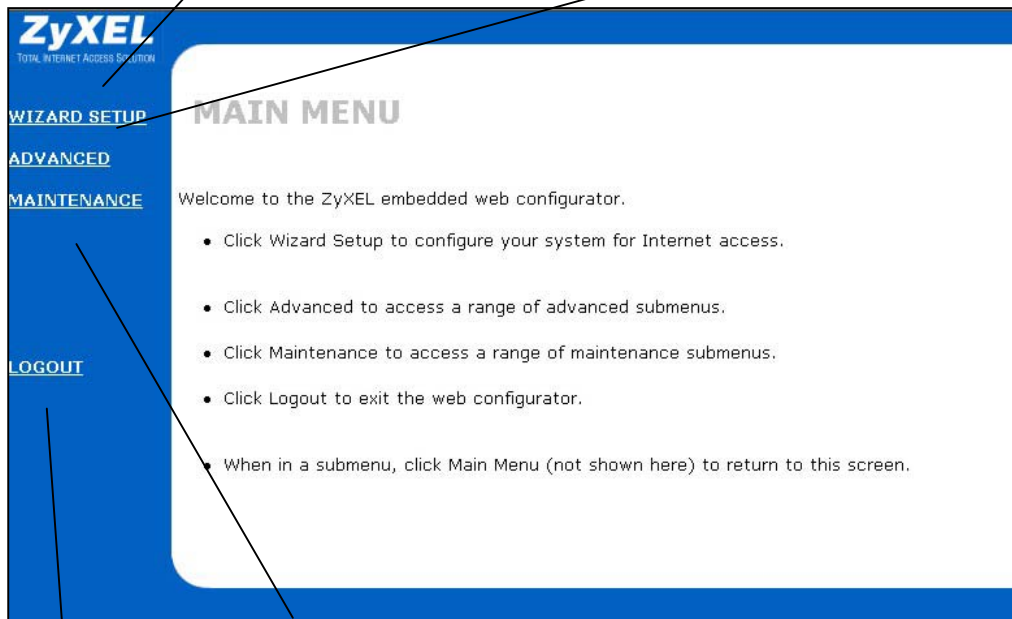
The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.

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

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

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

Click **ADVANCED** to configure advanced features such as **SYSTEM** (General Setup, Password), **WIRELESS** (Wireless, MAC Filter, Roaming, 802.1x, Local User Database and RADIUS), **IP**, **VLAN** and **Logs** (View reports and Log Settings).



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

Click **MAINTENANCE** to view information about your ZyAIR or upgrade configuration/firmware files. Maintenance includes **SYSTEM STATUS** (Statistics), **Wireless** (Association List and Channel Usage), **F/W** (firmware) **UPLOAD**, **CONFIGURATION** (Backup, Restore and Default).

Figure 2-2 The MAIN MENU Screen of the Web Configurator

Chapter 3

Wizard Setup

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

3.1 Wizard Setup Overview

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

3.1.1 Channel

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

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

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

3.1.2 ESS ID

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

3.1.3 WEP Encryption

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

3.2 Wizard Setup: General Setup

General Setup contains administrative and system-related information.

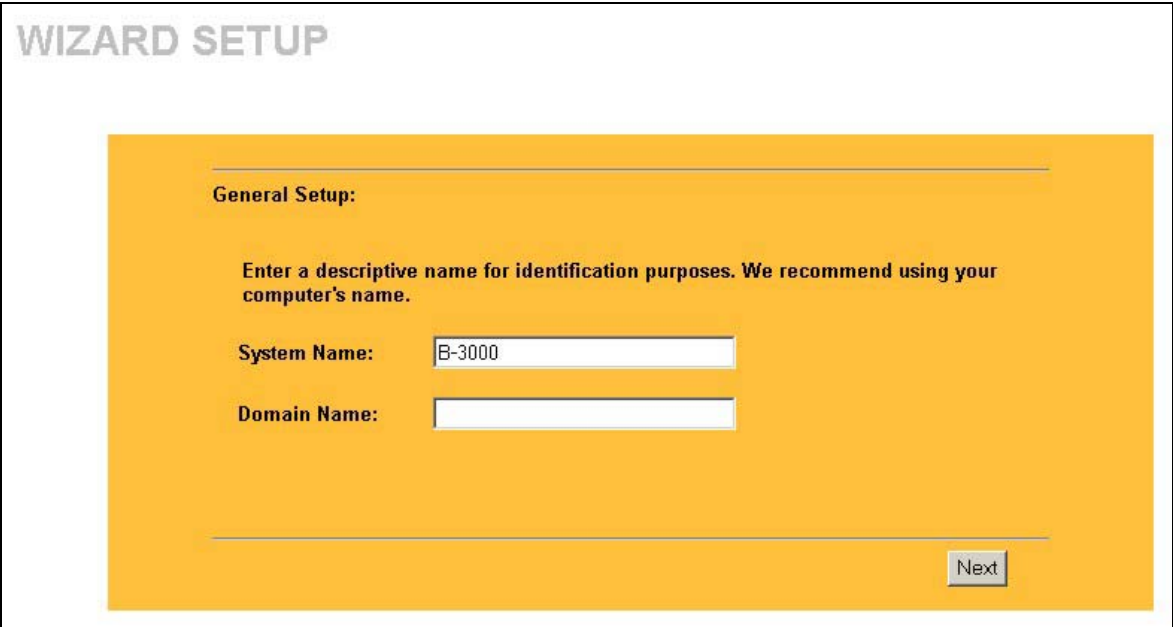


Figure 3-1 Wizard 1 : General Setup

The following table describes the labels in this screen.

Table 3-1 Wizard 1 : General Setup

LABEL	DESCRIPTION
System Name	<p>It is recommended you type your computer's "Computer name".</p> <ul style="list-style-type: none">➤ 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. <p>This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.</p>
Domain Name	<p>This is not a required field. Leave this field blank or enter the domain name here if you know it.</p>
Next	<p>Click Next to proceed to the next screen.</p>

3.3 Wizard Setup: Wireless LAN

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

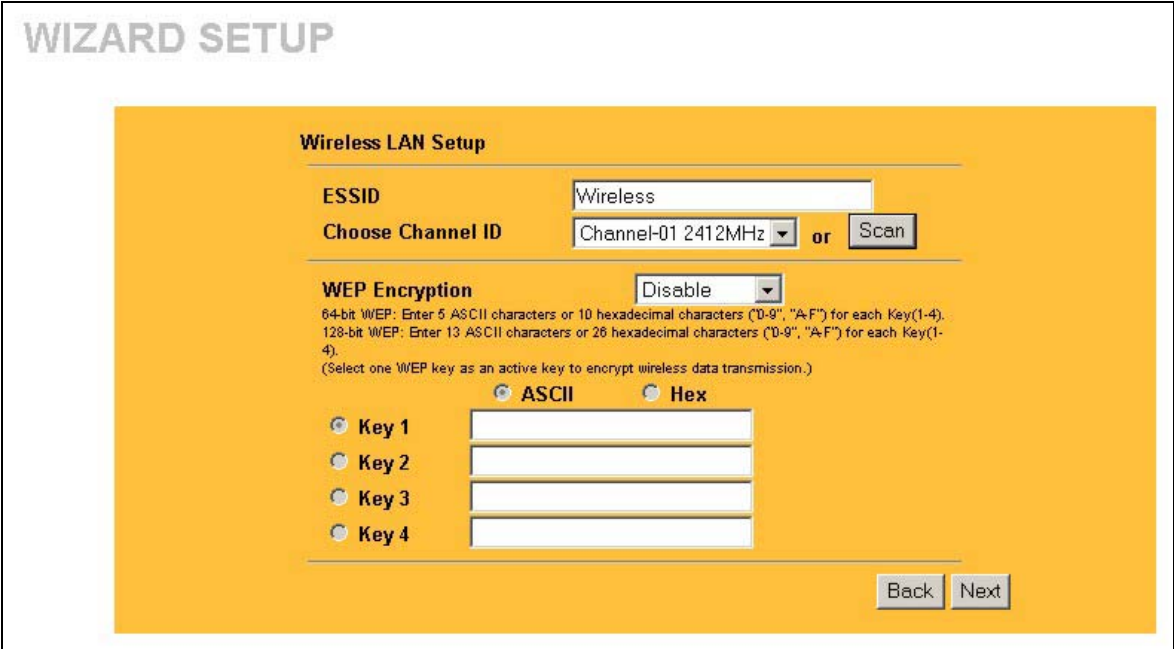


Figure 3-2 Wizard 2 : Wireless LAN Setup

The following table describes the labels in this screen.

Table 3-2 Wizard 2 : Wireless LAN Setup

LABEL	DESCRIPTION
Wireless LAN Setup	
ESSID	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 ESSID 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 Table 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.

Table 3-2 Wizard 2 : Wireless LAN Setup

LABEL	DESCRIPTION
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.
Next	Click Next to continue.
Back	Click Back to return to the previous screen.

3.4 Wizard Setup: IP Address

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

3.4.1 IP Address Assignment

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

Table 3-3 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.

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

3.4.2 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyAIR. 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.

WIZARD SETUP

IP Address Assignment

☐ Get automatically
☒ Use fixed IP address

IP Address
 IP Subnet Mask
 Gateway IP Address

Back Finish

Figure 3-3 Wizard 3 : IP Address Assignment

The following table describes the labels in this screen.

Table 3-4 Wizard 3 : IP Address Assignment

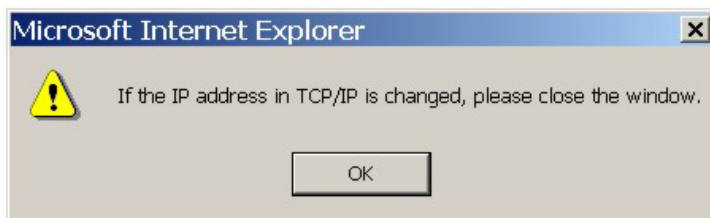
LABEL	DESCRIPTION
IP Address Assignment	
Get automatically	Select this option if your ZyAIR is using a dynamically assigned IP address from a DHCP server each time. <div> You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again. </div>
Use fixed IP address	Select 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. <div> If you changed the ZyAIR's IP address, you must use the new IP address if you want to access the web configurator again. </div>
IP Subnet Mask	Type the subnet mask.

Table 3-4 Wizard 3 : IP Address Assignment

LABEL	DESCRIPTION
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.
Back	Click Back to return to the previous screen.
Finish	Click Finish to proceed to complete the Wizard setup.

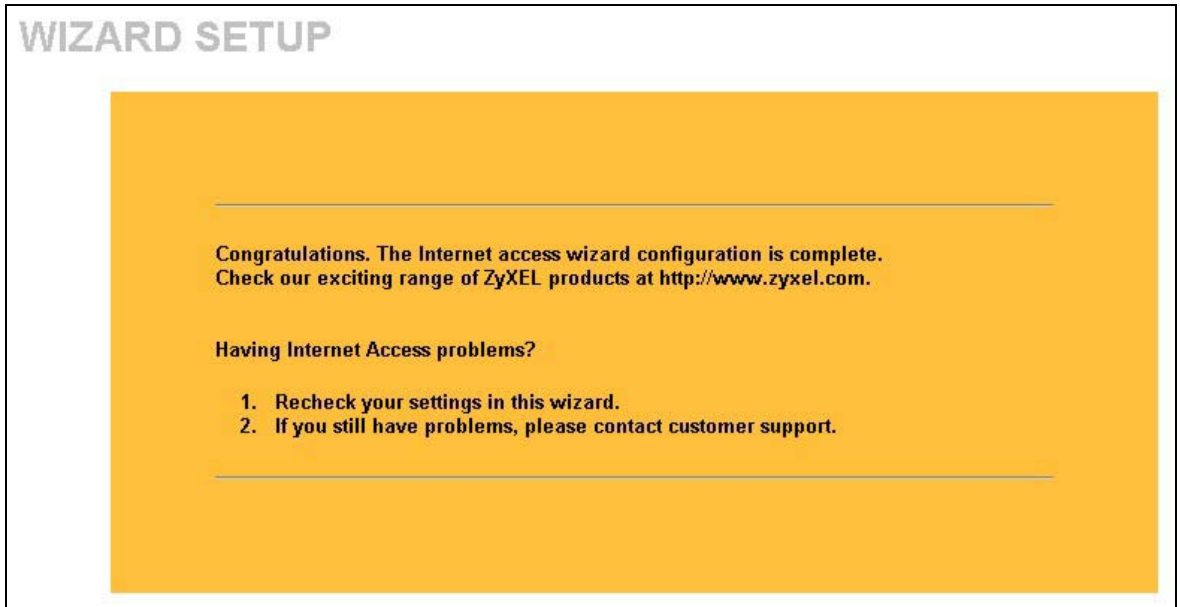
3.5 Basic Setup Complete

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



You have successfully set up the ZyAIR. A screen displays prompting you to close the web browser. Click **Yes**. Otherwise, click **No** and the congratulations screen shows next.





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

Part II:

SYSTEM, WIRELESS, VLAN AND IP

This part covers the information and web configurator screens of System, Wireless, VLAN and IP.

Chapter 4

System Screens

This chapter provides information on the System screens.

4.1 System Overview

This section provides information on general system setup.

4.2 Configuring General Setup

Click **ADVANCED** and then **SYSTEM** to open the **General** screen.

SYSTEM

General Password Time Setting

System Name B-3000

Domain Name

Administrator Inactivity Timer 5 (minutes, 0 means no timeout)

System DNS Servers

First DNS Server User-Defined 0.0.0.0

Second DNS Server None 0.0.0.0

Third DNS Server From ISP 0.0.0.0

Apply Reset

Figure 4-1 System General Setup

The following table describes the labels in this screen.

Table 4-1 System General Setup

LABEL	DESCRIPTION
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).
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.

4.3 Configuring Password

To change your ZyAIR's password (recommended), click **ADVANCED**, **SYSTEM** 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 in *Chapter 2* for details.

SYSTEM

General Password Time Setting

Old Password

New Password

Retype to Confirm

Apply Reset

Figure 4-2 Password

The following table describes the labels in this screen.

Table 4-2 Password

LABEL	DESCRIPTION
Old Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

4.4 Configuring Time Setting

To change your ZyAIR's time and date, click **ADVANCED**, **SYSTEM** 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.

SYSTEM

General

Password

Time Setting

Time Protocol

None

Time Server Address

Current Time (hh:mm:ss)

1

:

12

:

38

New Time (hh:mm:ss)

1

:

10

:

20

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)

Apply

Reset

Figure 4-3 Time Setting

The following table describes the labels in this screen.

Table 4-3 Time Setting

LABEL	DESCRIPTION
Time Protocol	<p>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.</p> <p>The main difference between them is the format.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>The default, NTP (RFC 1305), is similar to Time (RFC 868).</p> <p>Select None to enter the time and date manually.</p>

Table 4-3 Time Setting

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

Chapter 5

Wireless Configuration and Roaming

This chapter discusses how to configure Wireless and Roaming screens on the ZyAIR. Some features such as Multiple-ESS are not available on all models.

5.1 Wireless LAN Overview

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

5.1.1 IBSS

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



Figure 5-1 IBSS (Ad-hoc) Wireless LAN

5.1.2 BSS

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

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless 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.

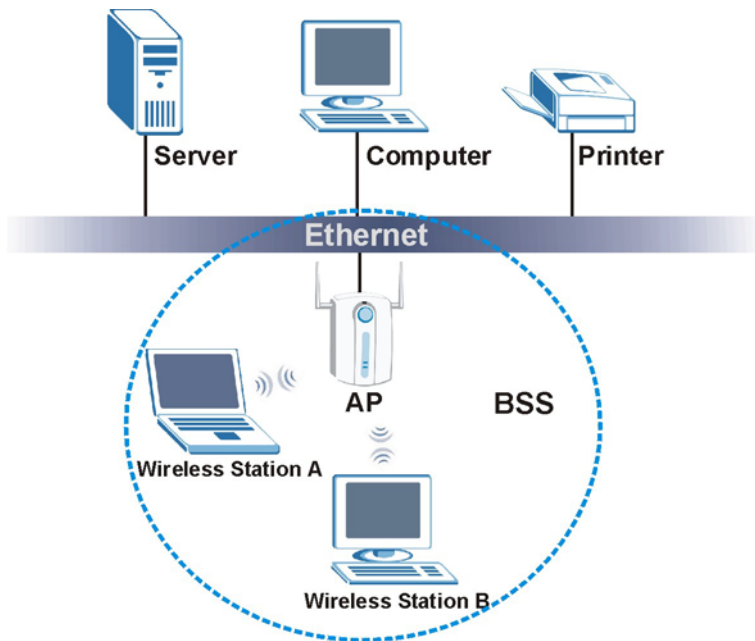


Figure 5-2 Basic Service set

5.1.3 ESS

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

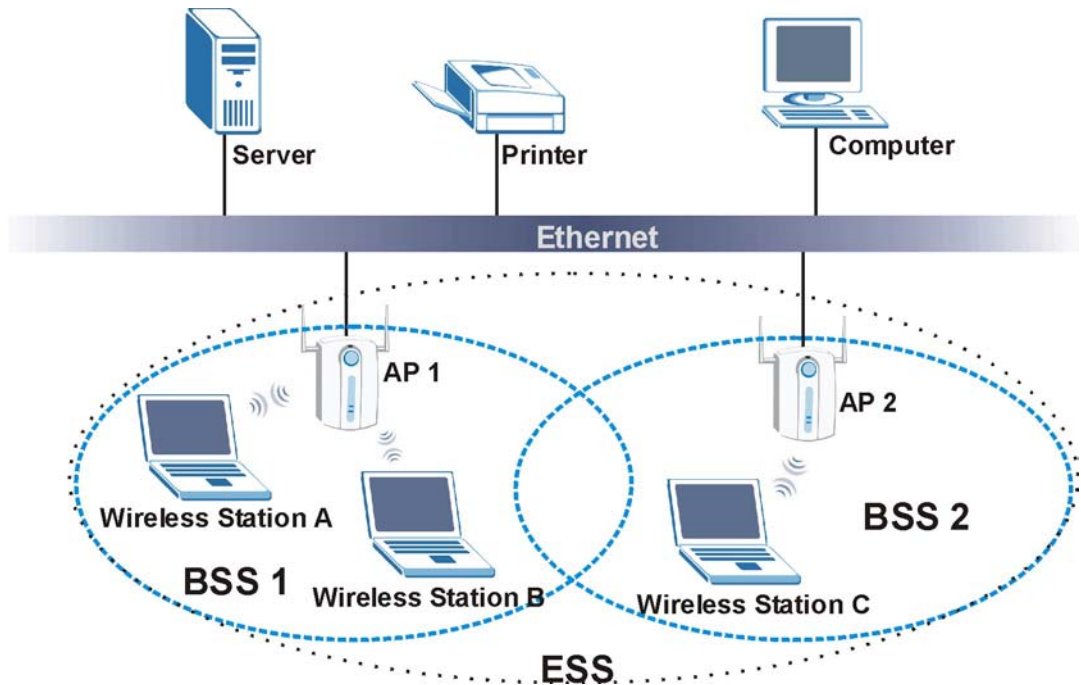


Figure 5-3 Extended Service Set

5.2 Wireless LAN Basics

Refer also to the *Wizard Setup* chapter for more background information on Wireless LAN features, such as channels.

5.2.1 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.

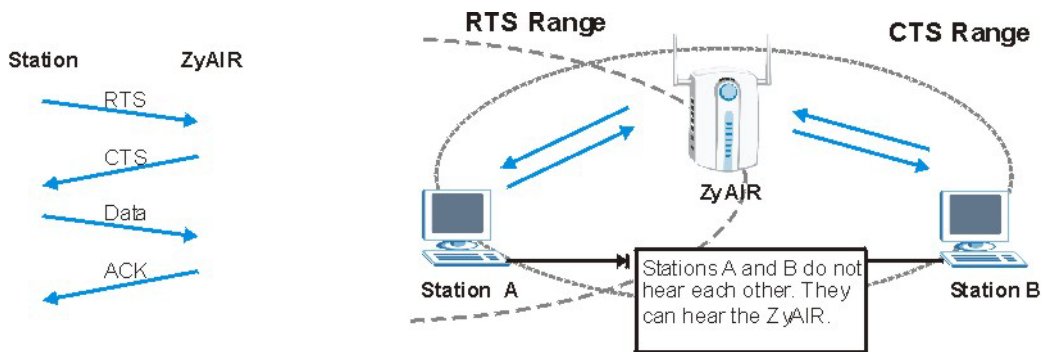


Figure 5-4 RTS/CTS

When station A sends data to the ZyAIR, 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.

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

5.2.2 Fragmentation Threshold

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

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

If the **Fragmentation Threshold** value is smaller than the **RTS/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.

5.3 Configuring Wireless

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

WIRELESS LAN

Wireless MAC Filter Roaming 802.1x Local User Database RADIUS

Operating Mode Access Point

ESSID Wireless

☐ Hide ESSID

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 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("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

Number of Wireless Stations Allowed 32 (1 ~ 32)

Output Power 17dBm (50mW)

Apply Reset

Figure 5-5 Wireless

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

Table 5-1 Wireless

LABEL	DESCRIPTION
Operating Mode	Select the operating mode from the drop-down list. Options are Access Point , Multiple ESS and Bridge . The screen changes when you select Multiple ESS or Bridge in this field. Refer to the <i>Multiple ESS and VLAN</i> chapter for more information on multiple ESS.
ESSID	(Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. <div>If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's ESSID 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.</div>
Hide ESSID	Select this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning using a site survey tool.
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 , WIRELESS 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 <i>Wizard Setup</i> 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	Enter a value between 0 and 2432. The default is 2432 .
Fragmentation Threshold	Enter a value between 256 and 2432. The default is 2432 . It is the maximum data fragment size that can be sent.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

See the *Wireless Security* chapter for information on the other labels in this screen.

5.4 Configuring Bridge

The ZyAIR can function as a wireless network bridge allowing you to wirelessly connect two wired network segments. You need to know the MAC address of the peer device, which also must be in bridge mode.

In the example below, Computers B and C will be able to communicate with Computer A through the ZyAIR bridges, forming a Wireless Distribution System (WDS).

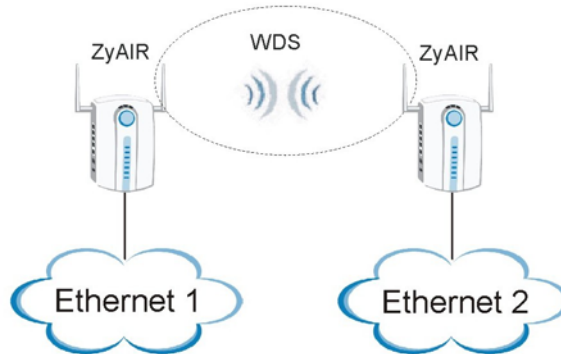


Figure 5-6 Bridging Example

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.

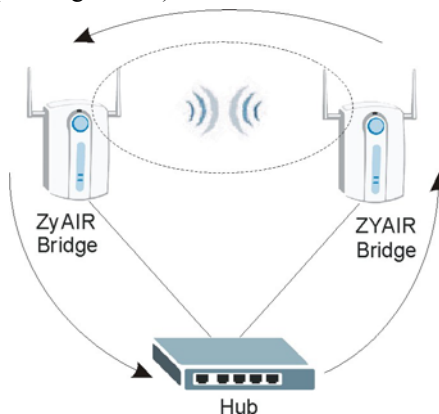


Figure 5-7 Bridge Loop: Two Bridges Connected to Hub

- 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.

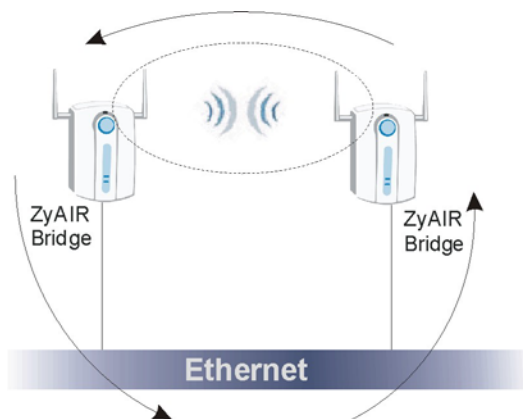


Figure 5-8 Bridge Loop: Bridge Connected to Wired LAN

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

Click **ADVANCED** and **WIRELESS**. Select **Bridge** in the **Operating Mode** drop-down list box to display the screen as shown.

WIRELESS LAN

Wireless

Operating Mode

Choose Channel ID

RTS/CTS Threshold

Fragmentation Threshold

Peer Bridge MAC Address

Bridge

Channel-06 2437MHz

2432 (0 ~ 2432)

2432 (256 ~ 2432)

00:00:00:00:00:00

or

Scan

WEP Encryption

Authentication Method

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("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 Breathing LED**

Output Power

Apply
Reset

Figure 5-9 Wireless : Bridge

The following table describes the bridge labels in this screen.

Table 5-2 Wireless : Bridge

LABEL	DESCRIPTION
Operating Mode	Select Bridge in this field to display the screen as shown in <i>Figure 5-9</i> .
Peer 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.

System Screens

5-9

5.5 Configuring Roaming

A wireless station is a device with an IEEE 802.11b compliant wireless adapters. 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 5-10*.

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.

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

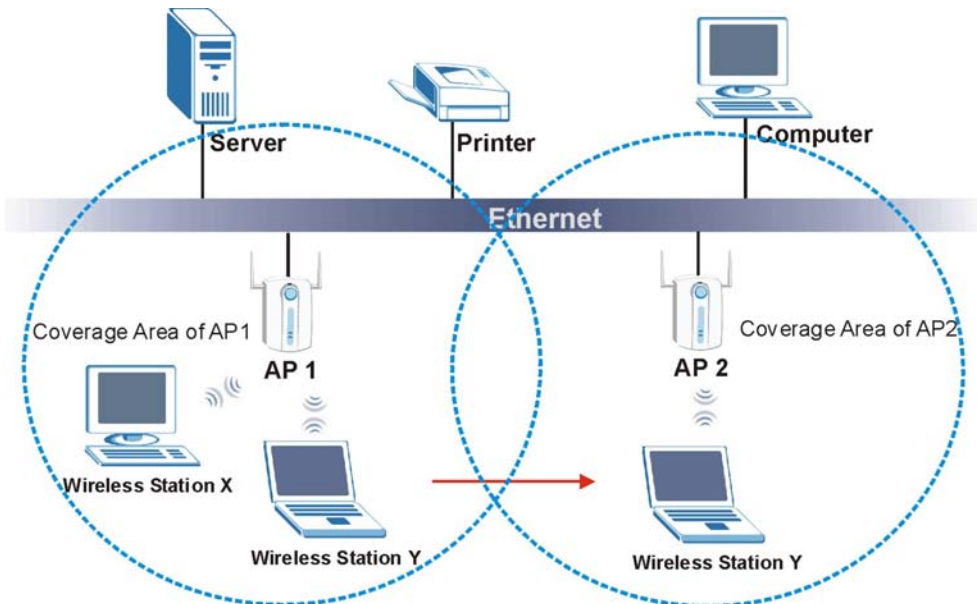


Figure 5-10 Roaming Example

The steps below describe the roaming process.

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

5.5.1 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 **ADVANCED**, **WIRELESS** and then the **Roaming** tab. The screen appears as shown.

WIRELESS LAN ROAMING

Wireless	MAC Filter	Roaming	802.1x	Local User Database	RADIUS
Roaming Configuration					
Active		No			
Port		16290			
		<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

Figure 5-11 Roaming

The following table describes the labels in this screen.

Table 5-3 Roaming

LABEL	DESCRIPTION
Active	<p>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.</p> <div data-bbox="288 341 1161 411">All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming.</div>
Port #	<p>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 16290. Make sure this port is not used by other services.</p>
Apply	<p>Click Apply to save your changes back to the ZyAIR.</p>
Reset	<p>Click Reset to begin configuring this screen afresh.</p>

Chapter 6

Wireless Security

This chapter describes how to use the MAC Filter, 802.1x, Local User Database and RADIUS to configure wireless security on your ZyAIR.

6.1 Wireless Security Overview

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

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

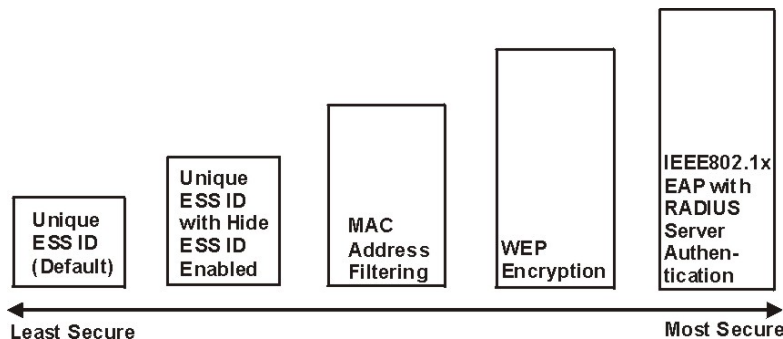


Figure 6-1 ZyAIR Wireless Security Levels

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 WEP Overview

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

6.2.1 Data Encryption

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

6.2.2 Authentication

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

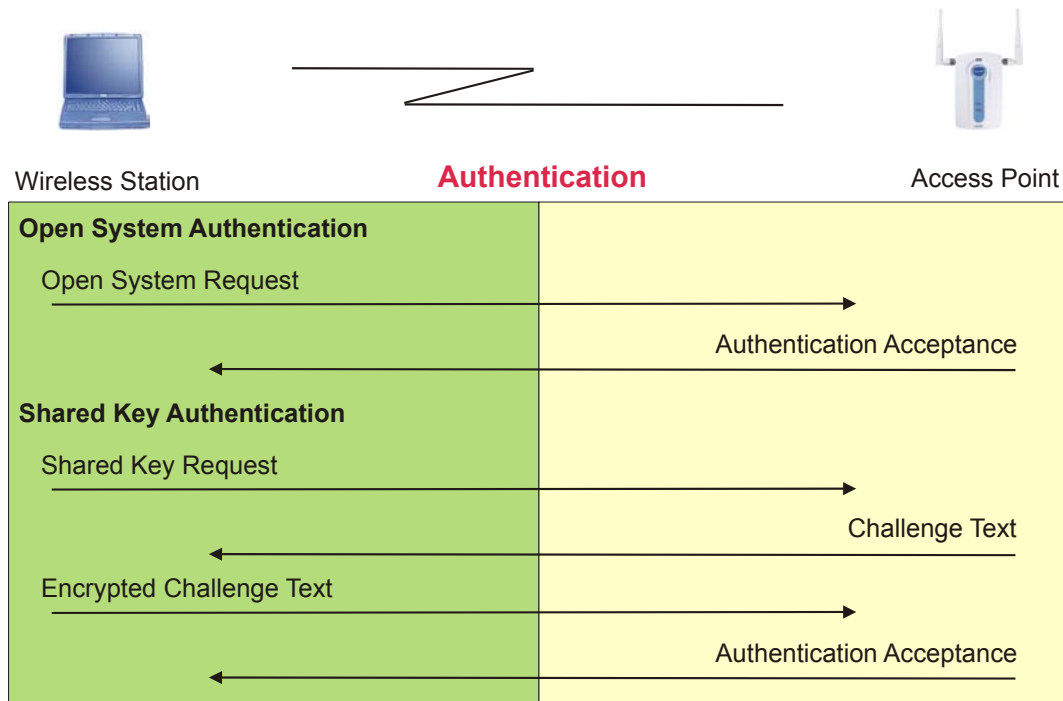


Figure 6-2 WEP Authentication Steps

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

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

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

6.3 Configuring WEP Encryption

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

WIRELESS LAN

Wireless | MAC Filter | Roaming | 802.1x | Local User Database | RADIUS

Operating Mode: Access Point

ESSID: Wireless

☐ Hide ESSID

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 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("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

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

Output Power: 17dBm (50mW)

Apply Reset

Figure 6-3 Wireless

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

Table 6-1 Wireless

LABEL	DESCRIPTION
WEP Encryption	Select Disable to allow wireless stations to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	Select Auto , Open System or Shared Key from the drop-down list box. This field is N/A if WEP is not activated. If WEP encryption is activated, the default setting is Auto .
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
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.
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.
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 11dBm (50mW) , 13dBm (32mW) , 15dBm (20mW) or 17dBm (12.6mW) .
Apply	Click Apply to save your changes back to the ZyAIR.

Table 6-1 Wireless

LABEL	DESCRIPTION
Reset	Click Reset to begin configuring this screen afresh.

6.4 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 **ADVANCED**, **WIRELESS** and then the **MAC Filter** tab. The screen appears as shown.

WIRELESS LAN

Wireless

MAC Filter

Roaming

802.1x

Local User Database

RADIUS

MAC Address Filter

Active

No

Filter Action

Allow Association

MAC Address

00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00
00:00:00:00:00:00	00:00:00:00:00:00

Apply

Reset

Figure 6-4 MAC Address Filter

The following table describes the labels in this screen.

Table 6-2 MAC Address Filter

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

Table 6-2 MAC Address Filter

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

6.5 802.1x Overview

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

6.6 Introduction to RADIUS

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

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

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

Types of RADIUS Messages

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

- **Access-Request**
Sent by an access point requesting authentication.

- **Access-Reject**

Sent by a RADIUS server rejecting access.

- **Access-Accept**

Sent by a RADIUS server allowing access.

- **Access-Challenge**

Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

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

- **Accounting-Request**

Sent by the access point requesting accounting.

- **Accounting-Response**

Sent by the RADIUS server to indicate that it has started or stopped accounting.

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

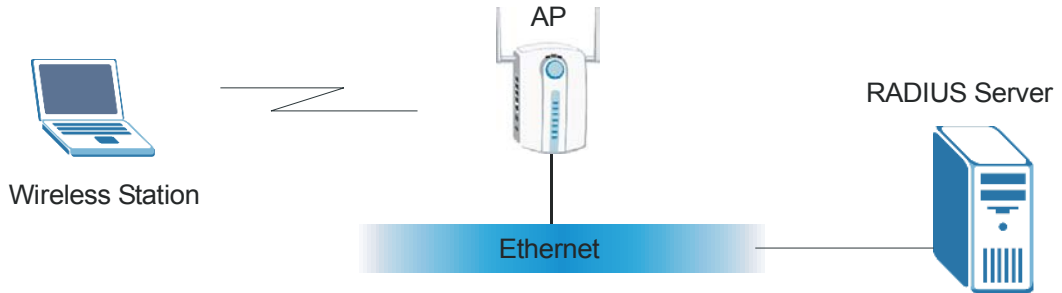
6.6.1 EAP Authentication Overview

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

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

Your ZyAIR supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database and RADIUS.

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

**Figure 6-5 EAP Authentication**

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

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

6.7 Dynamic WEP Key Exchange

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

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

To use Dynamic WEP, enable and configure the RADIUS server (see *section 6.11*) and enable Dynamic WEP Key Exchange in the 802.1x screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

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

6.8 Introduction to Local User Database

By storing user profiles locally on the ZyAIR, your ZyAIR is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

6.9 Configuring 802.1x

To change your ZyAIR's authentication settings, click **ADVANCED**, **WIRELESS** and then the **802.1x** tab. The screen appears as shown.

WIRELESS LAN

Wireless

MAC Filter

Roaming

802.1X

Local User Database

RADIUS

802.1X Authentication

Wireless Port Control

No Authentication Required

ReAuthentication Timer

1800

(In Seconds)

Idle Timeout

3600

(In Seconds)

Authentication Databases

Local User Database Only

Dynamic WEP Key Exchange

Disable

Apply

Reset

Figure 6-6 802.1x Authentication

The following table describes the labels in this screen.

Table 6-3 802.1x Authentication

LABEL	DESCRIPTION
Wireless Port Control	<p>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.</p> <p>No Authentication Required allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting.</p> <p>Authentication Required means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.</p> <p>No Access Allowed blocks all wireless stations access to the wired network.</p>
ReAuthentication Timer (in seconds)	<p>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.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <div data-bbox="413 695 1214 794"> <p>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p> </div>
Idle Timeout (in seconds)	<p>The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.</p> <p>This field is activated only when you select Authentication Required in the Wireless Port Control field. The default time interval is 3600 seconds (1 hour).</p>

Table 6-3 802.1x Authentication

LABEL	DESCRIPTION
Authentication Databases	<p>This field is activated only when you select Authentication Required in the Wireless Port Control field.</p> <p>The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local User Database Only to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password.</p> <p>Select RADIUS Only to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select Local first, then RADIUS to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server.</p> <p>Select RADIUS first, then Local to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.</p>
Dynamic WEP Key Exchange	<p>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.</p> <p>Select Disable to allow wireless stations to communicate with the access points without using dynamic WEP key exchange.</p> <p>Select 64-bit WEP or 128-bit WEP to enable data encryption.</p> <p>Up to 32 stations can access the ZyAIR when you configure dynamic WEP key exchange.</p>
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.
Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the ZyAIR for authentication.	

6.10 Configuring Local User Database

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

WIRELESS LAN

Wireless	MAC Filter	Roaming	802.1x	Local User Database	RADIUS
----------	------------	---------	--------	---------------------	--------

#	Active	User Name	Password
1	<input type="checkbox"/>		
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		
11	<input type="checkbox"/>		
12	<input type="checkbox"/>		
13	<input type="checkbox"/>		
14	<input type="checkbox"/>		
15	<input type="checkbox"/>		
16	<input type="checkbox"/>		
17	<input type="checkbox"/>		
18	<input type="checkbox"/>		
19	<input type="checkbox"/>		
20	<input type="checkbox"/>		
21	<input type="checkbox"/>		
22	<input type="checkbox"/>		
23	<input type="checkbox"/>		
24	<input type="checkbox"/>		
25	<input type="checkbox"/>		
26	<input type="checkbox"/>		
27	<input type="checkbox"/>		
28	<input type="checkbox"/>		
29	<input type="checkbox"/>		
30	<input type="checkbox"/>		
31	<input type="checkbox"/>		
32	<input type="checkbox"/>		

Apply Reset

Figure 6-7 Local User Database

The following table describes the labels in this screen.

Table 6-4 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 **ADVANCED**, **WIRELESS** and then the **RADIUS** tab. The screen appears as shown.

WIRELESS LAN

Wireless **MAC Filter** **Roaming** **802.1x** **Local User Database** **RADIUS**

Authentication Server

Active: (dropdown)

Server IP Address:

Port Number:

Shared Secret:

Accounting Server

Active: (dropdown)

Server IP Address:

Port Number:

Shared Secret:

Figure 6-8 RADIUS

The following table describes the labels in this screen.

Table 6-5 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 profile 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.
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.
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

This chapter is only applicable to the ZyAIR B-3000.

7.1 Wireless LAN Infrastructures

See the *Wizard Setup* and *Wireless Configuration* 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 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).

7.1.2 Notes on Multiple-ESS

1. A maximum of eight ESSs are allowed on one AP.
2. Each ESS has its own MAC filter set; see the MAC filter set section for more information.
3. 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.
4. You must use different WEP keys for different ESSs. If two stations have different ESSIDs (they are in different ESSs), but have the same WEP keys, they may hear each other's communications (but not communicate with each other).
5. When you enable Multi-ESS, ESSIDs are automatically hidden (so site survey tools cannot find other station ESSIDs).
6. Multi-ESS should not replace but rather be used in conjunction with 802.1x security.

7.1.3 Multiple ESS Example

In this 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.

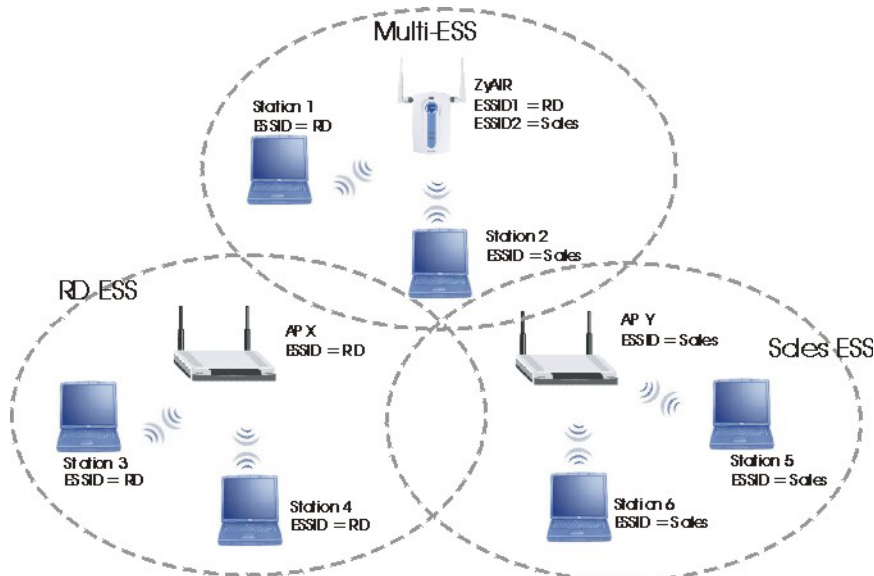


Figure 7-1 Multi-ESS Example

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.

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) with multi-ESS to extend the wireless logical grouping to the wired network. Each ESS is assigned a unique VLAN ID.

7.2.1 Management VLAN ID

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

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

7.2.2 Multi-ESS with VLAN Example

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

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

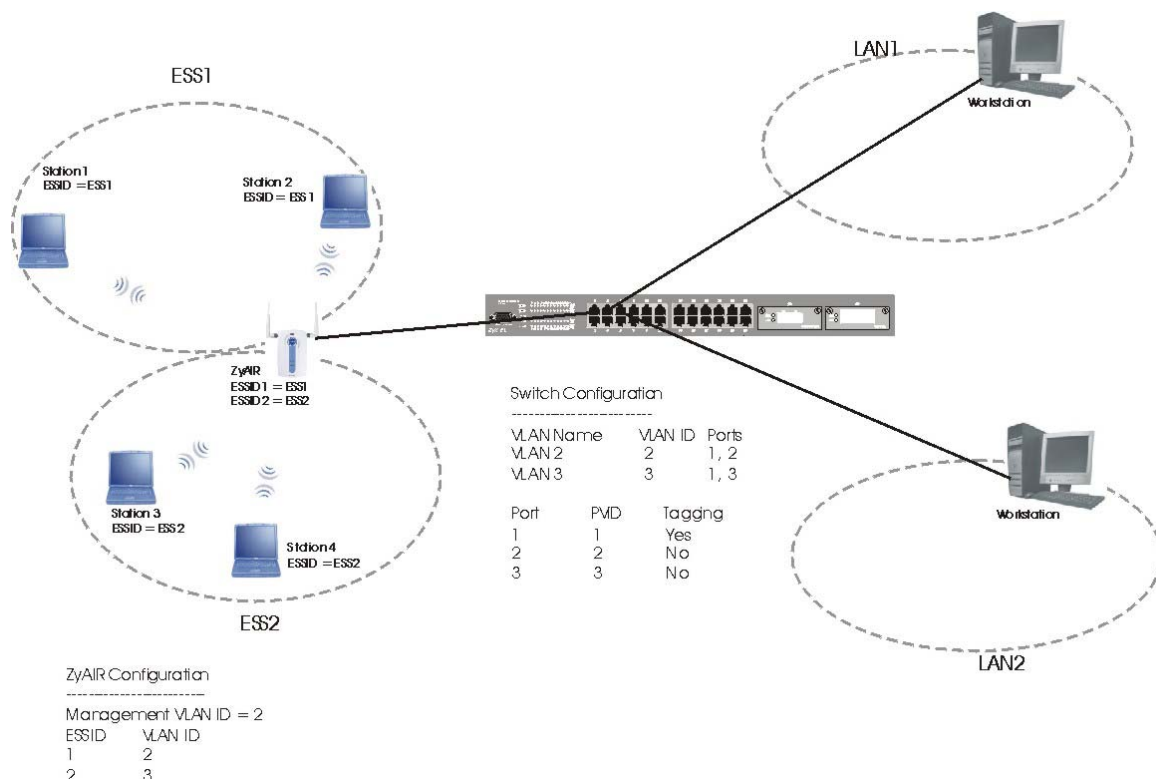


Figure 7-2 Multi-ESS with VLAN Example

7.3 Configuring Multiple ESS

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

WIRELESS LAN

Wireless

MAC Filter

Roaming

802.1x

Local User Database

RADIUS

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

Number of Wireless Stations Allowed

32

(1 ~ 32)

Output Power

17dBm (50mW)

Extended Service Sets (ESS) Summary

	#	ESSID	Active	VLAN ID
<input checked="" type="radio"/>	1	Wireless	Yes	1
<input checked="" type="radio"/>	2	CSOB1000	Yes	2
<input type="radio"/>	3	---	No	0
<input type="radio"/>	4	---	No	0
<input type="radio"/>	5	---	No	0
<input type="radio"/>	6	---	No	0
<input type="radio"/>	7	---	No	0
<input type="radio"/>	8	---	No	0

Edit

Delete

Apply

Reset

Figure 7-3 Wireless : Multiple ESS

The following table describes the labels in this screen.

Table 7-1 Wireless : Multiple ESS

LABEL	DESCRIPTION
Operating Mode	Select Multiple ESS in this field to display the screen as shown in <i>Figure 7-3</i> .
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, WIRELESS and then the Channel Usage tab to open the Channel Usage Table 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 <i>Wizard Setup</i> 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.
ESSID	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.
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.

7.3.1 Edit ESS

Click **Edit** on the **Wireless** screen.

EDIT ESS

ESSID

☐ Active

VLAN ID

0

(1 ~ 255)

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("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

Apply

Reset

Figure 7-4 Wireless : Edit ESS

The following table describes the labels in this screen.

Table 7-2 Wireless : Edit ESS

LABEL	DESCRIPTION
ESSID	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 255.
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.

7-6

Multiple ESS and VLAN

Table 7-2 Wireless : Edit ESS

LABEL	DESCRIPTION
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.

7.3.2 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.

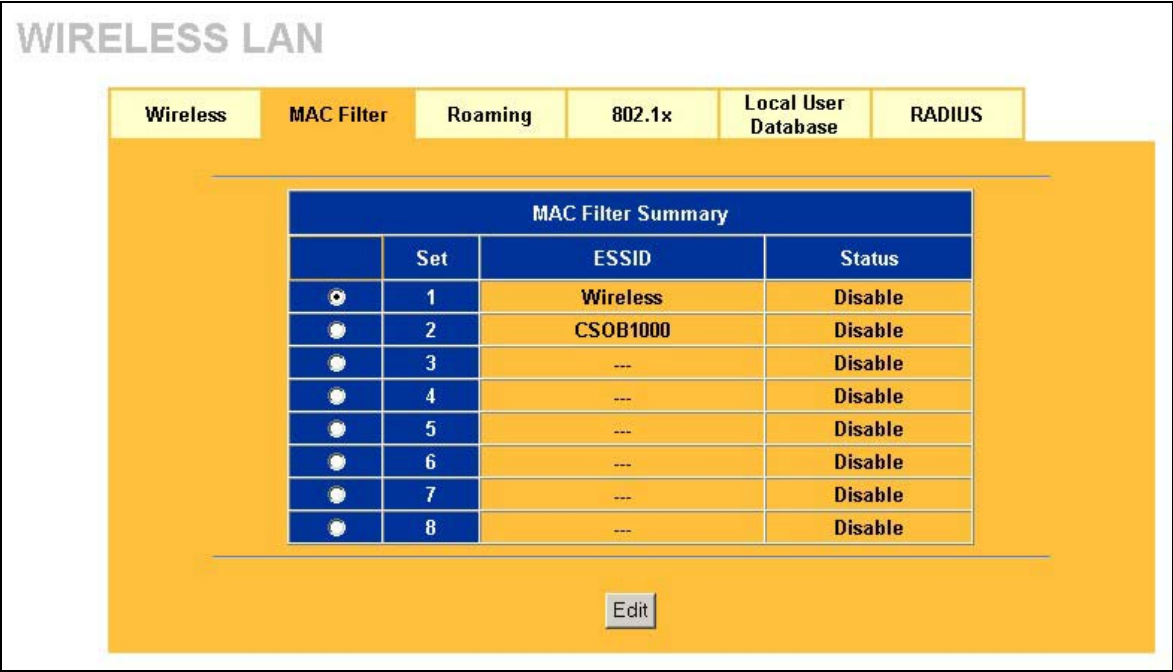


Figure 7-5 MAC Filter Summary

The following table describes the labels in this screen.

Table 7-3 MAC Filter Summary

LABEL	DESCRIPTION
Set	This is the index number of each ESS.
ESSID	This is the identification name of each ESS.
Status	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 <i>MAC Filter</i> section.

7.4 Configuring VLAN

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

VIRTUAL LAN

VLAN

☐ Enable VLAN Tagging

Management VLAN ID (1 ~ 255)

Apply Reset

Figure 7-6 VLAN

The following table describes the labels in this screen.

Table 7-4 VLAN

LABEL	DESCRIPTION
Enable VLAN Tagging	Select this check box to turn on VLAN tagging.
Management VLAN ID	Enter a number from 1 to 255 to define this VLAN group. At least one device in your network must belong to this VLAN group in order to manage the ZyAIR.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

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:

- IP address of 192.168.1.2
- 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 8-1 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.

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.

WAN SETUP

IP

IP Address Assignment

☐ Get automatically

☒ Use fixed IP address

IP Address

192.168.1.2

IP Subnet Mask

255.255.255.0

Gateway IP Address

0.0.0.0

Apply

Reset

Figure 8-1 IP Setup

The following table describes the labels in this screen.

Table 8-2 IP Setup

LABEL	DESCRIPTION
IP Address Assignment	

Table 8-2 IP Setup

LABEL	DESCRIPTION
Get automatically	Select this option if your ZyAIR is using a dynamically assigned IP address from a DHCP server each time. 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. 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.

Part III:

LOGS

This part provides information and configuration instructions for the logs.

Chapter 9

Logs 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 **ADVANCED** and then **LOGS** 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 *section 9.2*). 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.

#	Time	Message	Source	Destination	Notes ▲
1	01/01/2000 02:58:34	User login from WEB successfully	192.168.1.30		User:admin
2	01/01/2000 02:58:15	User login from SMT successfully			User:admin
3	01/01/2000 02:54:27	User login from WEB successfully	192.168.1.30		User:admin

Figure 9-1 View Log

The following table describes the labels in this screen.

Table 9-1 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 **ADVANCED, LOGS** 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.

LOGS

View Log

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)

UNIX Syslog:

☐ Active

Syslog IP Address:

0.0.0.0

(Server Name or IP Address)

Log Facility:

Local 1

Send Log:

Log Schedule:

When Log is Full

Day for Sending Log:

Sunday

Time for Sending Log:

0 (hour) : 0 (minute)

Log

☐ System Maintenance

☐ System Errors

☐ Access Control

☐ 802.1X

Send immediate alert

☐ System Errors

☐ Access Control

Apply

Reset

Figure 9-2 Log Settings

The following table describes the labels in this screen.

Table 9-2 Log Settings

LABEL	DESCRIPTION
Address Info	

Table 9-2 Log Settings

LABEL	DESCRIPTION
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.
UNIX Syslog	UNIX syslog sends a log to an external UNIX server used to store logs.
Active	Click Active to enable UNIX syslog.
Syslog IP Address	Enter the server name or the IP address of the syslog server that will log the CDR (Call Detail Record) and system messages.
Log Facility	Select the Local from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to your UNIX manual for more information.
Send Log	
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none">• Daily• Weekly• Hourly• When the Log is Full• None. <p>If the Weekly or the Daily option is selected, specify a time of day when the E-mail should be sent. If the Weekly option is selected, then also specify which day of the week the E-mail should be sent. If the When Log is Full option is selected, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	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.
Log	Select the categories of logs that you want to record.

Table 9-2 Log Settings

LABEL	DESCRIPTION
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.

Part IV:

MAINTENANCE

This part describes the Maintenance web configurator screens.

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.

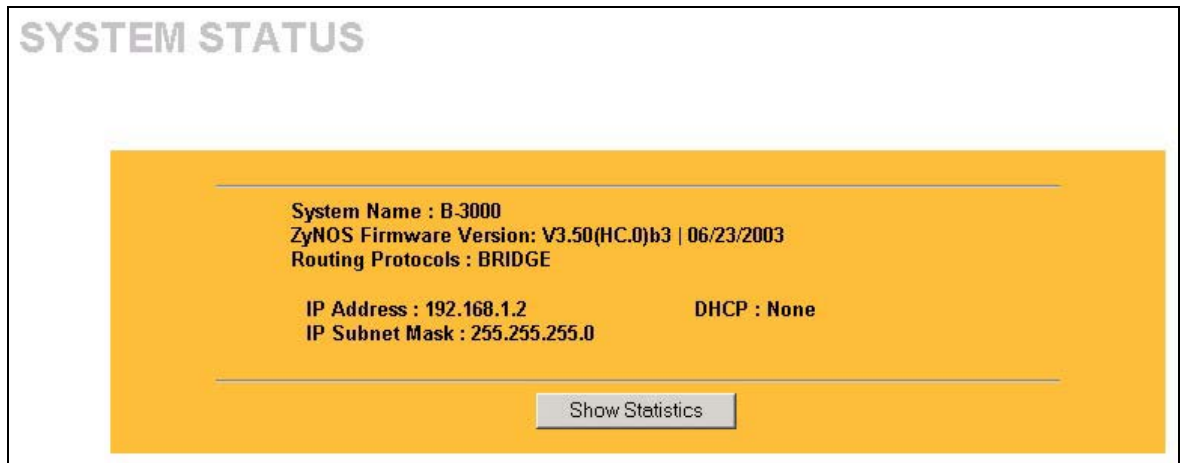


Figure 10-1 System Status

The following table describes the labels in this screen.

Table 10-1 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

Table 10-1 System Status

LABEL	DESCRIPTION
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocols	This shows the routing protocol – BRIDGE for which the ZyAIR is configured.
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 and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval** field is configurable.

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
Ethernet	100M/Full	1026	2319	0	0	248	0:28:38
Wireless	11M	714	0	0	128	0	0:28:38

System Up Time : 0:28:43

Poll Interval : sec

Figure 10-2 System Status: Show Statistics

The following table describes the labels in this screen.

Table 10-2 System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet or wireless port.

Table 10-2 System Status: Show Statistics

LABEL	DESCRIPTION
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	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 Wireless Screen

10.3.1 Association List

View the wireless stations that are currently associated to the ZyAIR in the **Association List** screen. Click **MAINTENANCE** and then **WIRELESS** to display the screen as shown next.

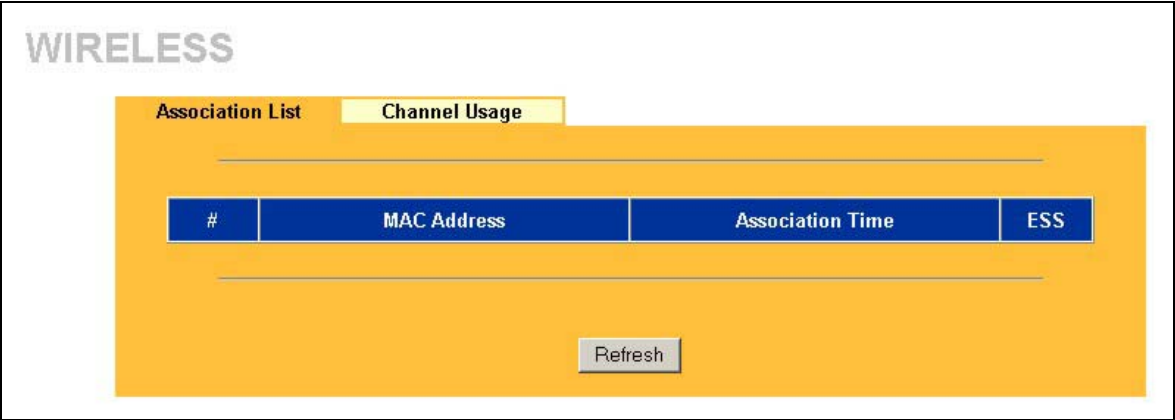


Figure 10-3 Association List

The following table describes the labels in this screen.

Table 10-3 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 identification name to which the wireless station is associated. This field is not available on all models.
Refresh	Click Refresh to reload the screen.

10.3.2 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**, **WIRELESS** and then the **Channel Usage** tab to display the screen shown next. Wait a moment while the ZyAIR compiles the information.

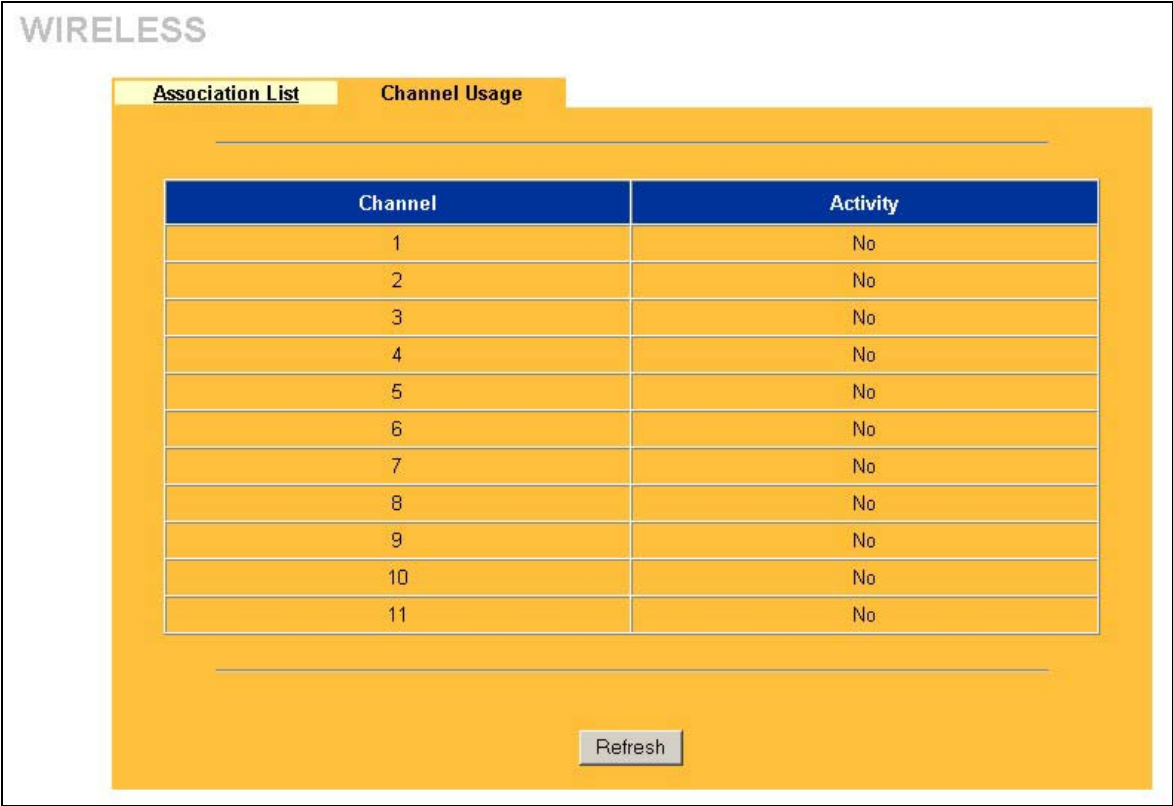


Figure 10-4 Channel Usage (ZyAIR B-1000)

The following table describes the labels in this screen.

Table 10-4 Channel Usage (ZyAIR B-1000)

LABEL	DESCRIPTION
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.
Activity	This field display Yes if the channel is used by another AP or Ad-hoc network within the ZyAIR’s transmission range.
Refresh	Click Refresh to reload the screen.

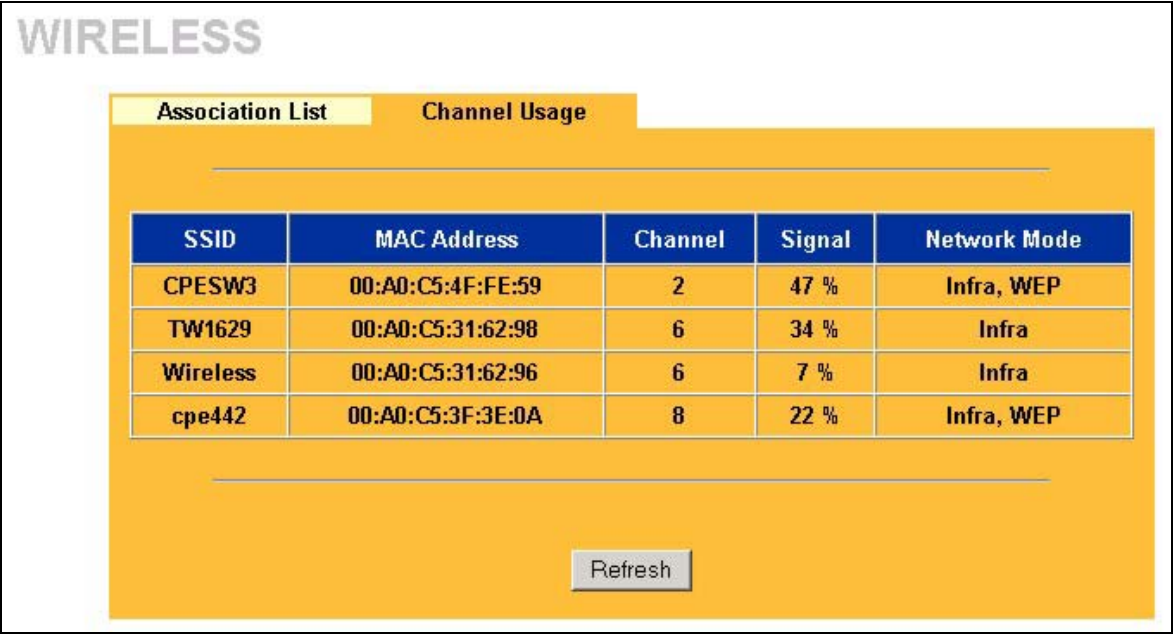


Figure 10-5 Channel Usage

The following table describes the labels in this screen.

Table 10-5 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 <i>Wireless Configuration and Roaming</i> chapter for more information on basic service sets (BSS) and extended service sets (ESS).
MAC Address	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Signal	This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference.

Table 10-5 Channel Usage

LABEL	DESCRIPTION
Network Mode	<p>“Network mode” in this screen refers to your wireless LAN infrastructure (refer to the <i>Wireless LAN</i> chapter) and WEP setup.</p> <p>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.</p>
Refresh	Click Refresh to reload the screen.

10.4 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.

FIRMWARE UPLOAD

To upgrade the internal router 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 router after upgrading.

File Path:

Figure 10-6 Firmware Upload

The following table describes the labels in this screen.

Table 10-6 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.

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

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

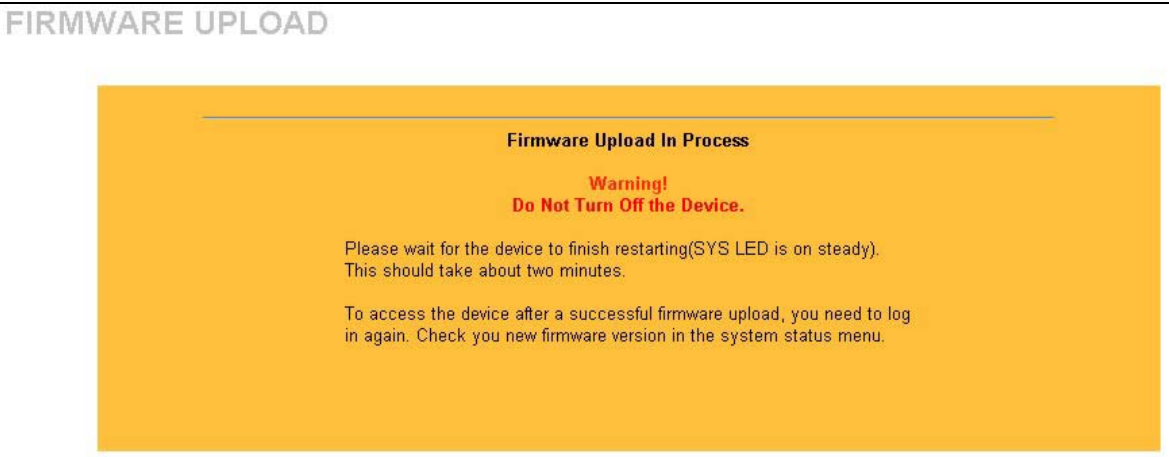


Figure 10-7 Firmware Upload In Process

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

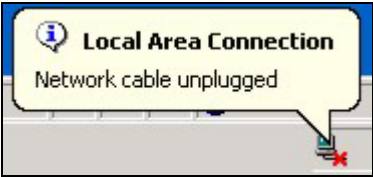


Figure 10-8 Network Temporarily Disconnected

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

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

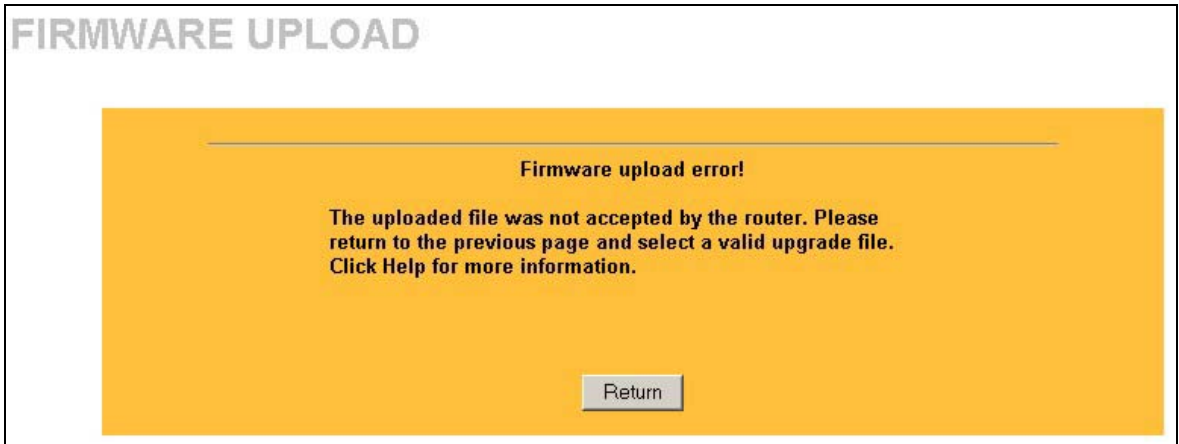


Figure 10-9 Firmware Upload Error

10.5 Configuration Screen

The web configurator uses TFTP to transfer files. See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

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

10.5.1 Backup Configuration

Backup Configuration allows you to backup (save) the current system (ZyAIR) configuration to your computer. Backup is highly recommended once your ZyAIR is functioning properly.

Click **Backup** to save your current ZyAIR configuration to your computer.

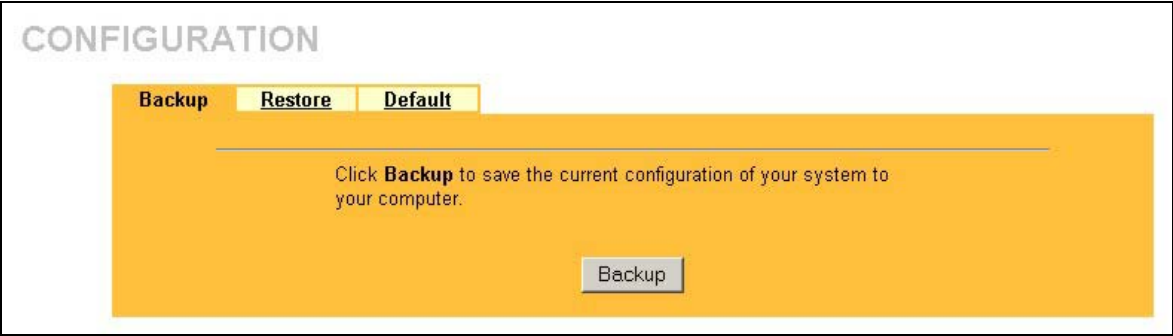


Figure 10-10 Backup Configuration

10.5.2 Restore Configuration

Restore configuration replaces your ZyAIR's current configuration with a previously saved configuration. Restore files (usually) have a .ROM extension, e.g., "zyair.rom". The system reboots automatically after the file transfer is complete and uses the configured values in the file.

WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyAIR. When the Restore Configuration process is complete, the ZyAIR will automatically restart.



Figure 10-11 Restore Configuration

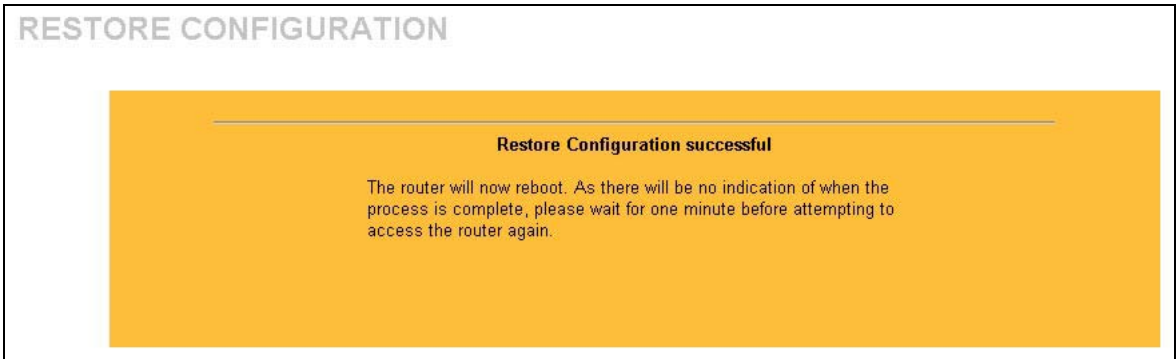
The following table describes the labels in this screen.

Table 10-7 Restore Configuration

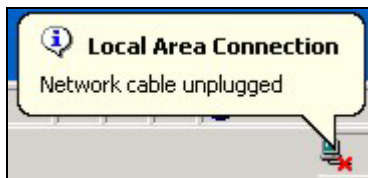
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin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

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

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

**Figure 10-12 Configuration Upload Successful**

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

**Figure 10-13 Network Temporarily Disconnected**

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

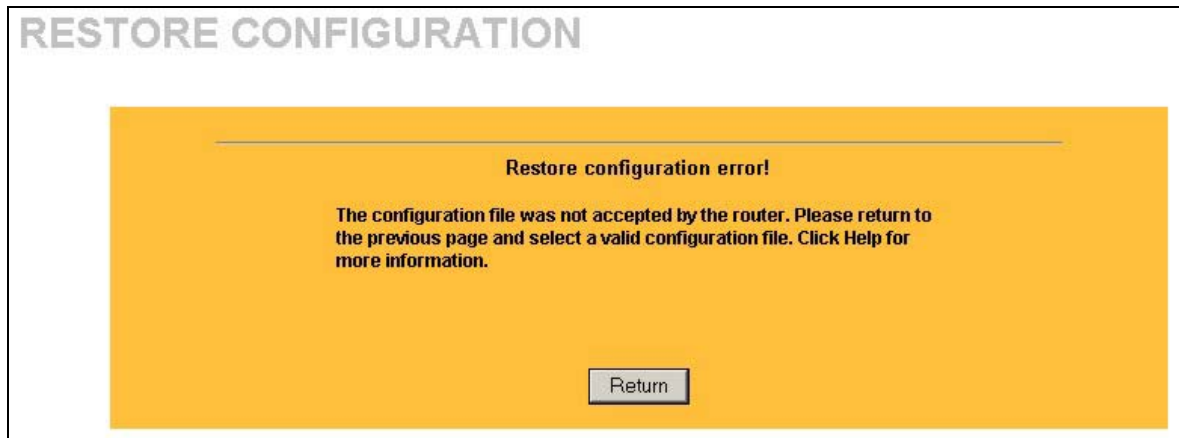


Figure 10-14 Configuration Upload Error

10.5.3 Back to Factory Defaults

Clicking 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. This will erase all configurations that you have applied.

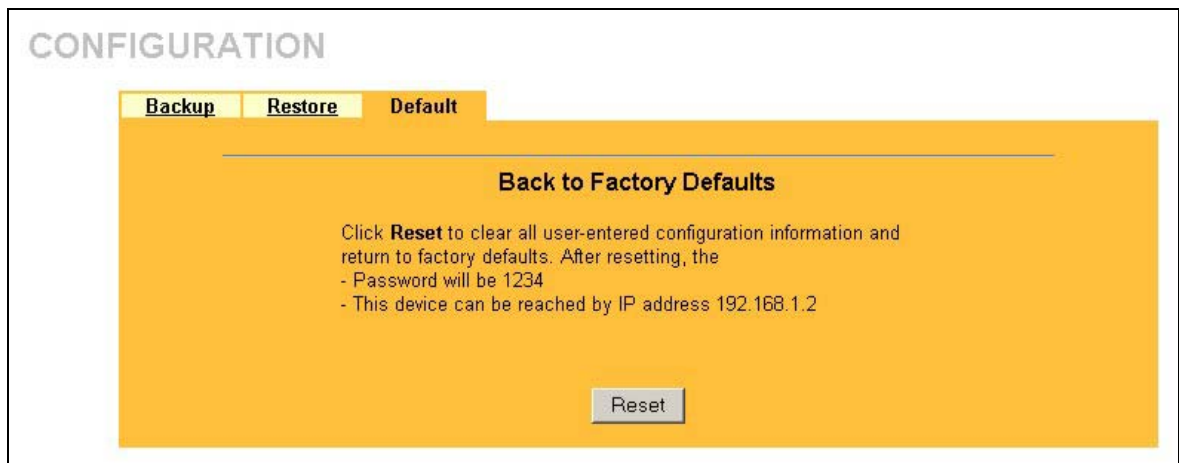


Figure 10-15 Back to Factory Default

The following warning screen will appear.

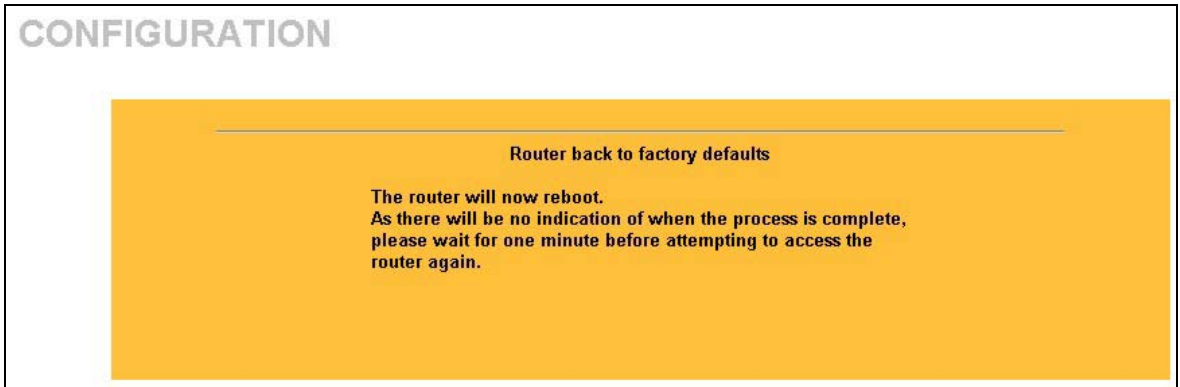


Figure 10-16 Reset Warning Message

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

Part V:

SMT CONFIGURATION

This part contains SMT (System Management Terminal) configuration and background information for features only configurable by SMT.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

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.

- Step 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**.
- Step 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.

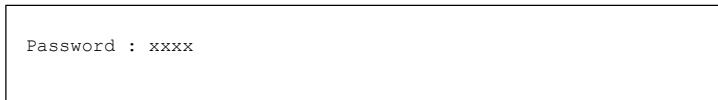


Figure 11-1 Login Screen

- Step 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.

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

```
Menu 23.1 - System Security - Change Password

Old Password= ****
New Password= ?
Retype to confirm= ?

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 11-2 Menu 23.1 System Security : Change Password

- Step 4.** Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].
- Step 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 Menu Overview Example

We use the ZyAIR B-3000 SMT menus in this guide as an example. The SMT menus for your model may vary slightly for different ZyAIR models.

The following figure gives you an example overview of the various SMT menu screens for your ZyAIR B-3000.

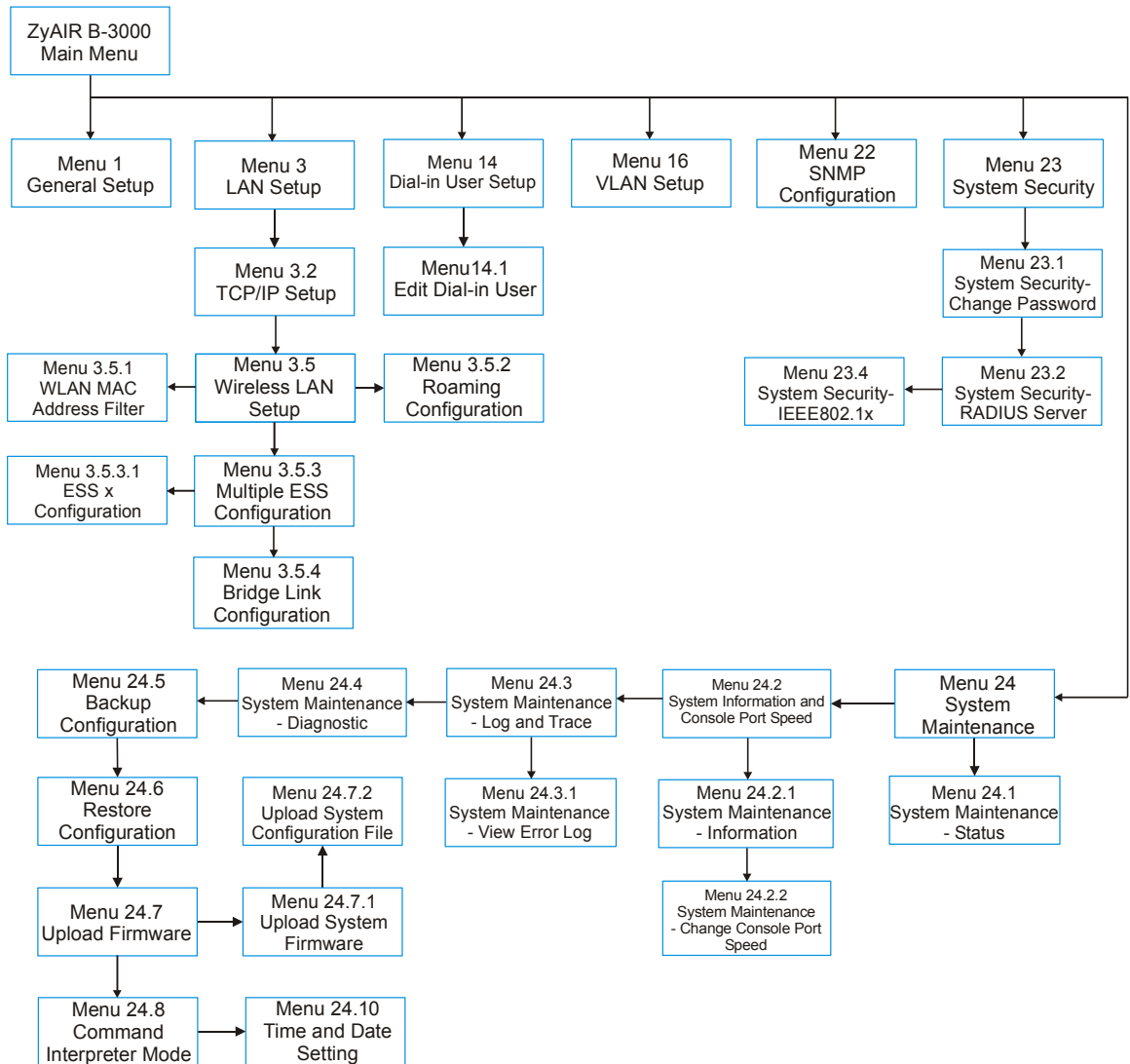


Figure 11-3 ZyAIR B-3000 SMT Menu Overview Example

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 11-1 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].
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.

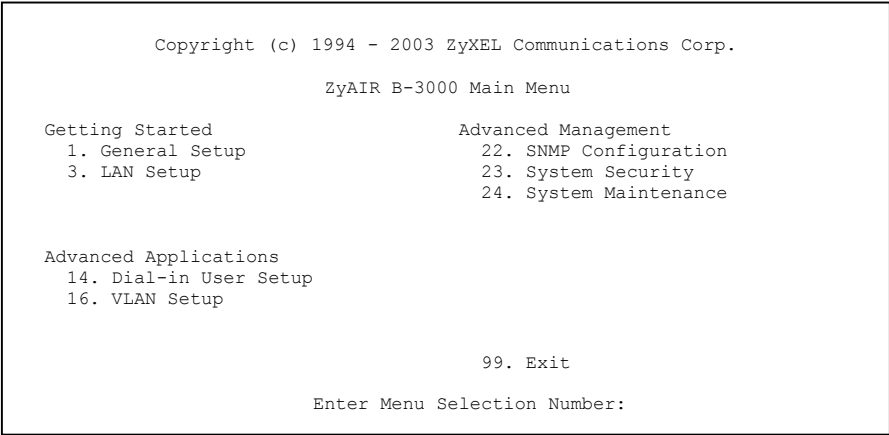


Figure 11-4 ZyAIR B-3000 SMT Main Menu

11.4.1 System Management Terminal Interface Summary

Table 11-2 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 tagging.
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.
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

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

Menu 1 - General Setup

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

Press ENTER to Confirm or ESC to Cancel:

Figure 12-1 Menu 1 General Setup

Step 2. Fill in the required fields. Refer to the following table for more information about these fields.

Table 12-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
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.	B-3000
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.	From DHCP
IP Address	Enter the IP addresses of the DNS servers. This field is available when you select User-Defined in the field above.	N/A
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.

```
Menu 3 - LAN Setup

2. TCP/IP Setup

5. Wireless LAN Setup

Enter Menu Selection Number:
```

Figure 13-1 Menu 3 LAN Setup

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:

```
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

Press ENTER to Confirm or ESC to Cancel:
```

Figure 13-2 Menu 3.2 TCP/IP Setup

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

Table 13-1 Menu 3.2 TCP/IP Setup

FIELD	DESCRIPTION	EXAMPLE
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	192.168.1.2
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.	255.255.255.0
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.

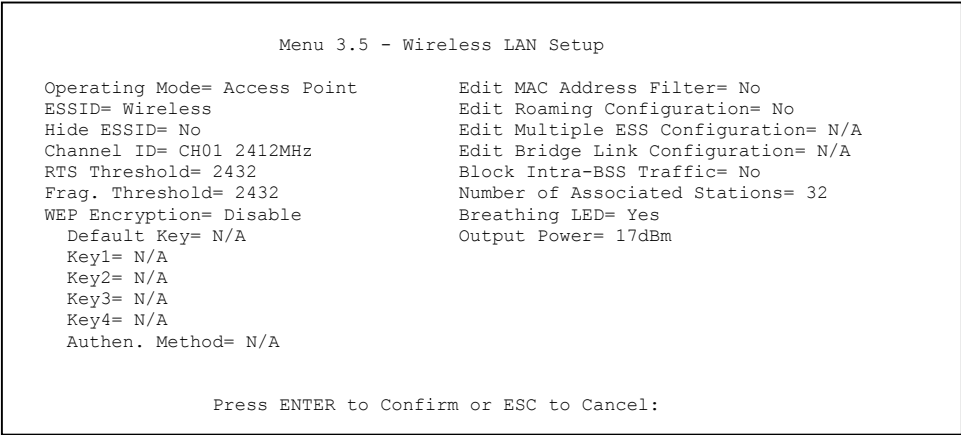


Figure 13-3 Menu 3.5 Wireless LAN Setup

The following table describes the fields in this menu.

Table 13-2 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXMAPLE
Operating Mode	Press [SPACE BAR] and select Access Point , Multiple ESS or Bridge . This field is not available on all models.	Access Point
ESSID	The ESSID (Extended Service Set IDentity) identifies the AP the wireless station is to associate to. Wireless stations associating to the AP must have the same ESSID. Enter a descriptive name up to 32 printable 7-bit ASCII characters. This field is only available when you select Access Point in the Operating Mode field.	Wireless
Hide ESSID	Press [SPACE BAR] and select Yes to hide the ESSID in the outgoing data frame so an intruder cannot obtain the ESSID through passive scanning.	No
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.	CH01 2412MHz
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.	2432
Frag. Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.	2432

Table 13-2 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION	EXMAPLE
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.	Disable
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.	1
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"). <div style="border: 1px solid black; padding: 5px; text-align: center;">Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key.</div>	0x12345ab cde
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 .	Auto
Block Intra-BSS Traffic	Press [SPACE BAR] to select Yes or No and press [ENTER].	
Number of Association Stations	Enter the number of association stations. The number should be from 1 to 32.	
Breathing LED	Press [SPACE BAR] to select Yes or No and press [ENTER].	
Output Power	Press [SPACE BAR] to select 11dBm , 13dBm , 15dBm or 17dBm and press [ENTER].	17dBm
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.

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

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

Menu 3.5 - Wireless LAN Setup

Operating Mode= Access Point	Edit MAC Address Filter= Yes
ESSID= Wireless	Edit Roaming Configuration= No
Hide ESSID= No	Edit Multiple ESS Configuration= N/A
Channel ID= CH01 2412MHz	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	
Key2= N/A	
Key3= N/A	
Key4= N/A	
Authen. Method= N/A	

Press ENTER to Confirm or ESC to Cancel:

Figure 13-4 Menu 3.5 Wireless LAN Setup

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

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

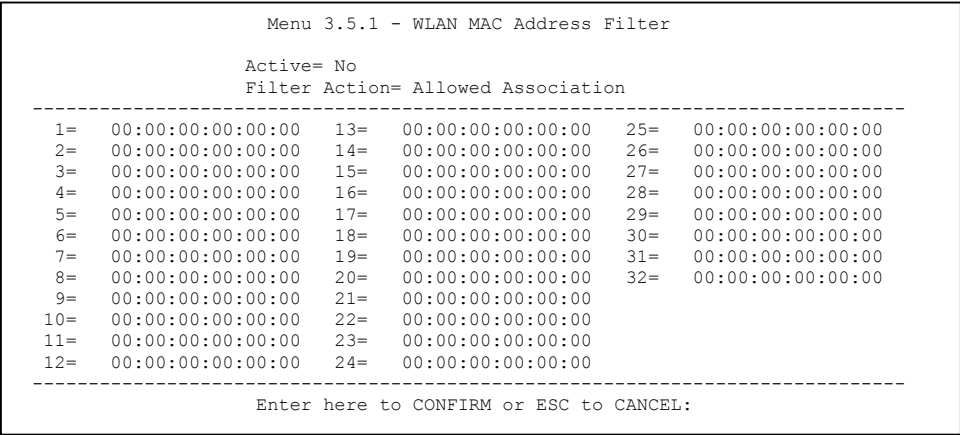


Figure 13-5 Menu 3.5.1 WLAN MAC Address Filter

The following table describes the fields in this menu.

Table 13-3 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.

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

```
Menu 3.5 - Wireless LAN Setup

Operating Mode= Access Point      Edit MAC Address Filter= No
ESSID= Wireless                  Edit Roaming Configuration= Yes
Hide ESSID= No                   Edit Multiple ESS Configuration= N/A
Channel ID= CH01 2412MHz         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
    Key2= N/A
    Key3= N/A
    Key4= N/A
    Authen. Method= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Figure 13-6 Menu 3.5 Wireless LAN Setup

- Step 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.

```
Menu 3.5.2 - Roaming Configuration

Active= Yes
Port #= 16290

Press ENTER to Confirm or ESC to Cancel:
```

Figure 13-7 Menu 3.5.2 Roaming Configuration

The following table describes the fields in this menu.

Table 13-4 Menu 3.5.2 Roaming Configuration

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select Yes to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet.
Port #	Type the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is 16290 . 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.	

13.3.3 Configuring Multiple ESS (for ZyAIR B-3000 only)

Follow the steps below to configure Multiple ESS on your ZyAIR.

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

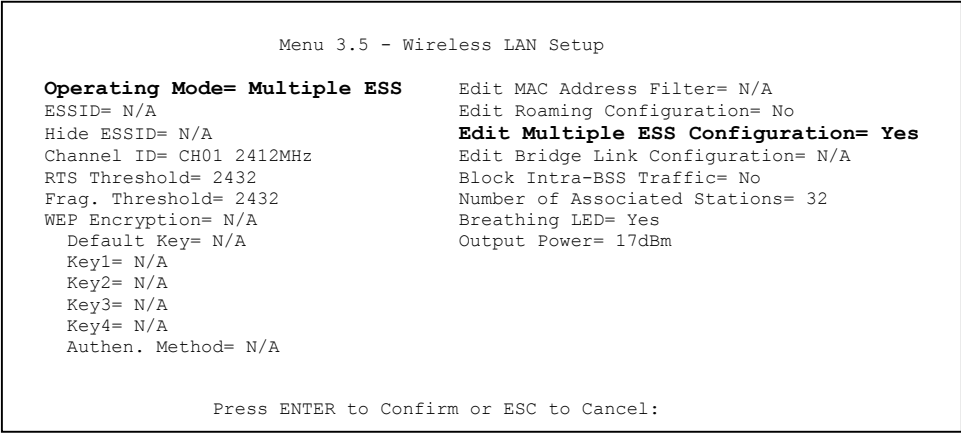


Figure 13-8 Menu 3.5 Wireless LAN Setup

- Step 3.** In the **Operating Mode** field, press [SPACE BAR] to select **Multiple ESS** and press [ENTER].
- Step 4.** Move the cursor to the **Edit Multiple ESS Configuration** field. Press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.3 – Multiple ESS Configuration** displays as shown next.

Menu 3.5.3 - Multiple ESS Configuration				
Number	ESSID	Active	VLAN ID	MAC Filter
1	Wireless	Y	1	Disable
2	CSOB1000	Y	2	Disable
3		N	0	Disable
4		N	0	Disable
5		N	0	Disable
6		N	0	Disable
7		N	0	Disable
8		N	0	Disable

WEP= 64-bit WEP				
Action= Edit				
ESS= 0				
Press ENTER to Confirm or ESC to Cancel:				

Figure 13-9 Menu 3.5.3 Multiple ESS Configuration

The following table describes the fields in this menu.

Table 13-5 Menu 3.5.3 Multiple ESS Configuration

FIELD	DESCRIPTION	EXAMPLE
WEP	Press [SPACE BAR] to select 64-bit WEP or 128-bit WEP .	
Action	Press [SPACE BAR] to select Edit or Delete .	
ESS	Type the ESS number and press [ENTER] to configure an extended service set.	
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.		

Configuring an Extended Service Set

Move the cursor to the **ESS** field in the menu 3.5.3. Type the ESS number and press [ENTER] to configure that service set. **Menu 3.5.3.1 – ESS x Configuration** displays as shown next

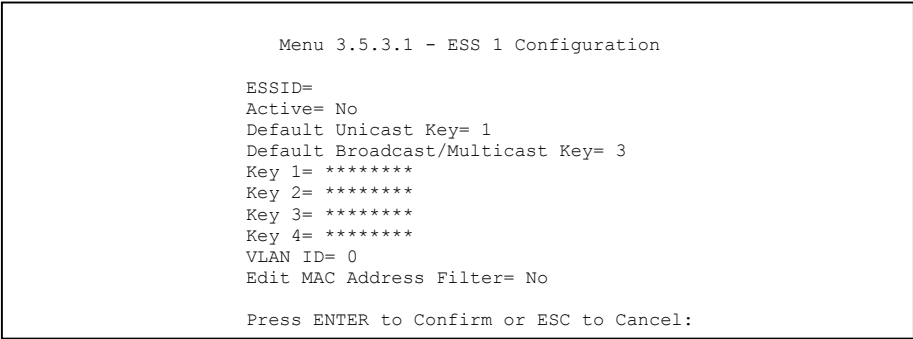


Figure 13-10 Menu 3.5.3.1 ESS x Configuration

The following table describes the fields in this menu.

Table 13-6 Menu 3.5.3.1 ESS x Configuration

FIELD	DESCRIPTION
ESSID	Enter the descriptive name up to 32 alphanumeric characters for identification. This field is case sensitive.
Active	Press [SPACE BAR] to select Yes or No and press [ENTER].
Default Unicast Key	Key 1 or key 2 is used to encrypt unicast transmissions.
Default Broadcast Key	Key 3 or key 4 is used to encrypt multicast/broadcast transmissions.
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission.</p> <p>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").</p> <p>If you chose 128-bit WEP in the WEP Encryption field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <div>Enter “0x” before the key to denote a hexadecimal key. Don’t enter “0x” before the key to denote an ASCII key.</div>
VLAN ID	Enter a number from 1 to 255.

Table 13-6 Menu 3.5.3.1 ESS x Configuration

FIELD	DESCRIPTION
Edit MAC Address Filter	Each service set has its own MAC address filter. Refer to <i>MAC Address Filter</i> section for details.
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.	

13.3.4 Configuring Bridge Link (for ZyAIR B-3000 only)

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

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

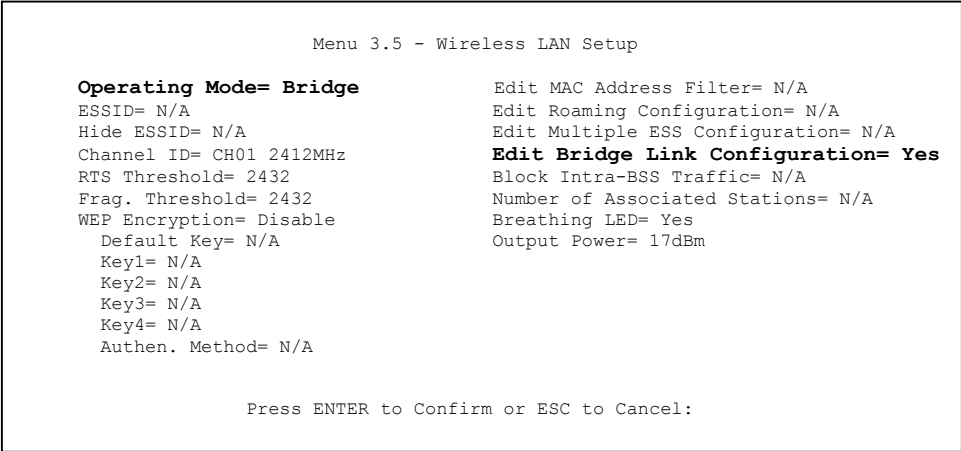


Figure 13-11 Menu 3.5 Wireless LAN Setup

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

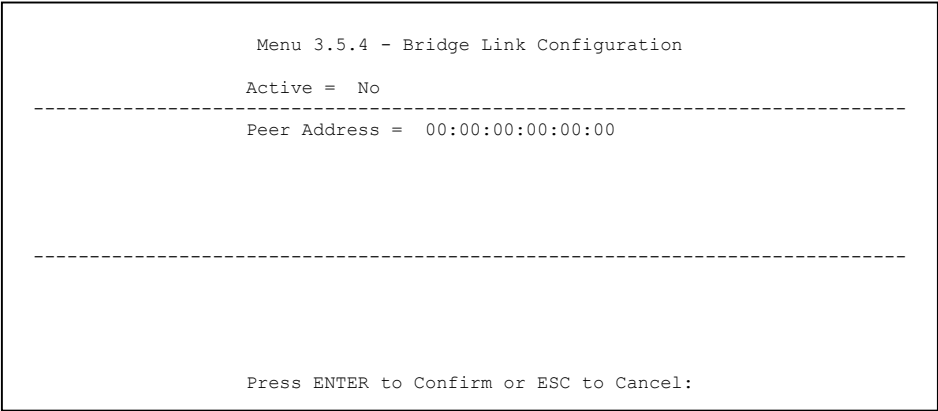


Figure 13-12 Menu 3.5.4 Bridge Link Configuration

The following table describes the fields in this menu.

Table 13-7 Menu 3.5.4 Bridge Link Configuration

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select Yes or No and press [ENTER].	No
Peer Address	Type the MAC address of peer device in valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.	
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.

Step 1. From the main menu, enter 14 to display **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:

Figure 14-1 Menu 14- Dial-in User Setup

Step 2. Type a number and press [ENTER] to edit the user profile.

Menu 14.1 - Edit Dial-in User

User Name= test

Active= Yes

Password= *****

Press ENTER to Confirm or ESC to Cancel:

Figure 14-2 Menu 14.1- Edit Dial-in User

The following table describes the fields in this screen.

Table 14-1 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

VLAN Setup

This chapter explains VLAN Setup menu 16. Refer to the Multiple-ESS and VLAN chapter for background information on VLAN. This chapter is not available on all models.

15.1 VLAN Setup

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

```
Menu 16 - VLAN Setup

VLAN Tagging= No
Native VLAN ID= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Figure 15-1 Menu 16 VLAN Setup

The following table describes the fields in this menu.

Table 15-1 Menu 16 VLAN Setup

FIELD	DESCRIPTION	EXAMPLE
VLAN Tagging	To enable VLAN tagging, press [SPACE BAR] to select Yes and press [ENTER].	No
Native VLAN ID	Enter a number from 1 to 255. This field is activated only when you select Yes in the VLAN Tagging field.	
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 16

SNMP Configuration

This chapter explains SNMP Configuration menu 22.

16.1 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.

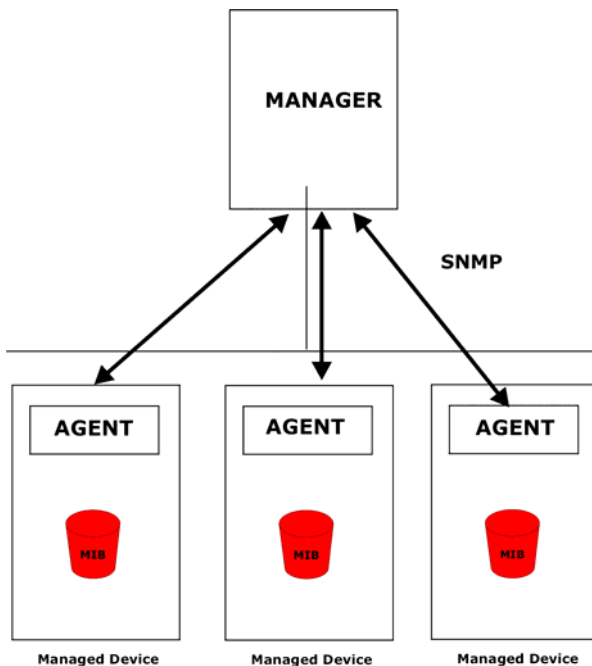


Figure 16-1 SNMP Management Model

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.

16.2 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.

16.3 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.

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:

Figure 16-2 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 16-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the Get Community , which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the Set Community , which is the password for incoming Set requests from the management station.	public
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.	0.0.0.0
Trap:		
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	public
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
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.		

16.4 SNMP Traps

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

Table 16-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (power on).
2	warmStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (software reboot).
3	linkUp (<i>defined in RFC-1215</i>)	A trap is sent when the port is up.
4	authenticationFailure (<i>defined in RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (<i>defined in RFC-1215</i>)	A trap is sent when the port is down.

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

Table 16-3 Ports and Interface Types

PHYSICAL PORT/ENCAP	INTERFACE TYPE
LAN port(s)	enet0
Wireless port	enet1
PPPoE encap	pppoe
1483 encap	mpoa
Ethernet encap	enet-encap
PPPoA	ppp

Chapter 17

System Security

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

17.1 System Security

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

17.1.1 System Password

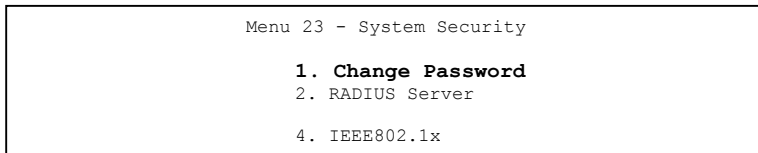


Figure 17-1 Menu 23 System Security

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

17.1.2 Configuring External RADIUS Server

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

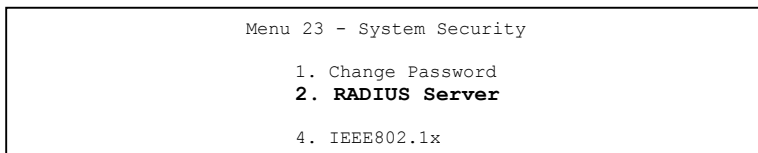


Figure 17-2 Menu 23 System Security

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

```
Menu 23.2 - System Security - RADIUS Server

Authentication Server:
Active= No
Server Address= 10.11.12.13
Port #= 1812
Shared Secret= ?

Accounting Server:
Active= No
Server Address= 10.11.12.13
Port #= 1813
Shared Secret= ?

Press ENTER to Confirm or ESC to Cancel:
```

Figure 17-3 Menu 23.2 System Security : RADIUS Server

The following table describes the fields in this menu.

Table 17-1 Menu 23.2 System Security : RADIUS Server

FIELD	DESCRIPTION	EXAMPLE
Authentication Server		
Active	Press [SPACE BAR] to select Yes and press [ENTER] to enable user authentication through an external authentication server.	No
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.	10.11.12.13
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.	1812
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.	No
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	10.11.12.13

Table 17-1 Menu 23.2 System Security : RADIUS Server

FIELD	DESCRIPTION	EXAMPLE
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.	1813
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.		

17.1.3 802.1x

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.

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

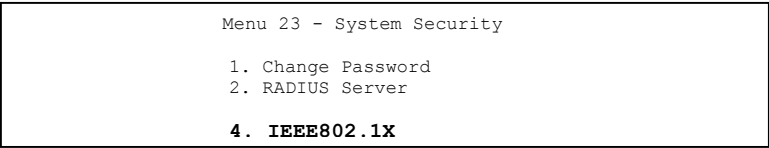


Figure 17-4 Menu 23 System Security

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

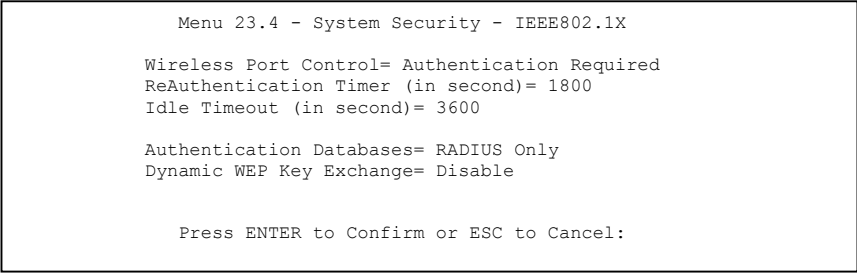


Figure 17-5 Menu 23.4 System Security : IEEE802.1x

The following table describes the fields in this menu.

Table 17-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	<p>Press [SPACE BAR] and select a security mode for the wireless LAN access.</p> <p>Select No Authentication Required to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting.</p> <p>Selecting Authentication Required means wireless stations have to enter usernames and passwords before access to the wired network is allowed.</p> <p>Select No Access Allowed to block all wireless stations access to the wired network.</p>
ReAuthentica- tion Timer (in seconds)	<p>Specify how often a wireless station has to re-enter username and password to stay connected to the wired network.</p> <p>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).</p>
Idle Timeout	<p>The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.</p> <p>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).</p>

Table 17-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Authentication Databases	<p>This field is activated only when you select Authentication Required in the Wireless Port Control field.</p> <p>The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this field to decide which database the ZyAIR should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local User Database Only to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password.</p> <p>Select RADIUS Only to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select Local first, then RADIUS to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server.</p> <p>Select RADIUS first, then Local to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.</p>
Dynamic WEP Key Exchange	<p>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.</p> <p>Select Disable to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange.</p> <p>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.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

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

Chapter 18

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.

```
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:
```

Figure 18-1 Menu 24 System Maintenance

18.1 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.

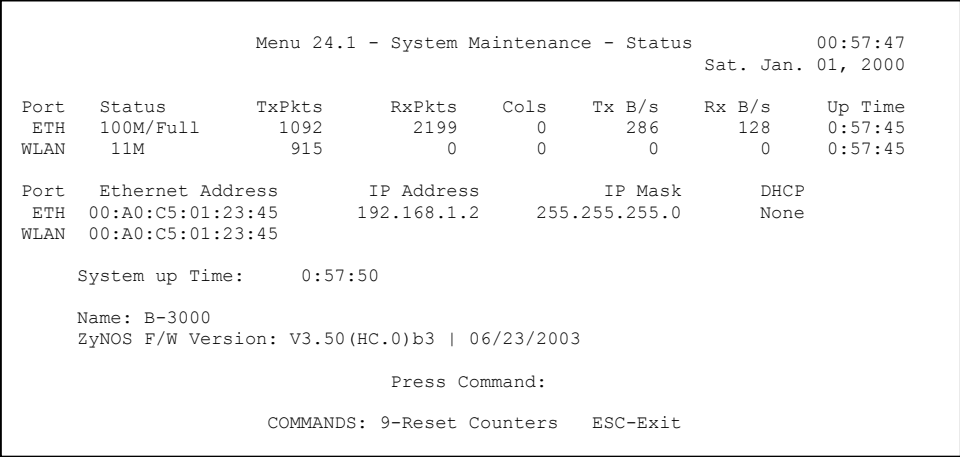


Figure 18-2 Menu 24.1 System Maintenance : Status

The following table describes the fields present in this menu.

Table 18-1 Menu 24.1 System Maintenance : Status

FIELD	DESCRIPTION
Port	This is the port type. Port types are: Ethernet and Wireless
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.

Table 18-1 Menu 24.1 System Maintenance : Status

FIELD	DESCRIPTION
System Up Time	This is the time the ZyAIR is up and running from the last reboot.

18.2 System Information

To get to the System Information:

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

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

Please enter selection:
```

Figure 18-3 Menu 24.2 System Information and Console Port Speed

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

18.2.1 System Information

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

```
Menu 24.2.1 - System Maintenance - Information

Name: B-3000
Routing: BRIDGE
ZyNOS F/W Version: V3.50(HC.0)b3 | 06/23/2003
Country Code: 255

LAN
Ethernet Address: 00:A0:C5:01:23:45
IP Address: 192.168.1.2
IP Mask: 255.255.255.0
DHCP: None

Press ESC or RETURN to Exit:
```

Figure 18-4 Menu 24.2.1 System Information : Information

The following table describes the fields in this menu.

Table 18-2 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.
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.	

18.2.2 Console Port Speed

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

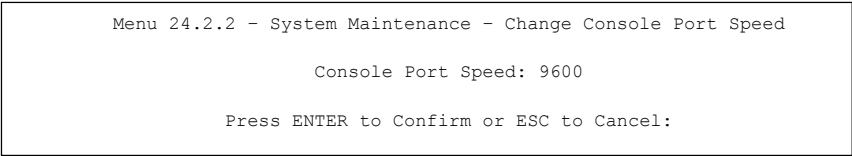


Figure 18-5 Menu 24.2.2 System Maintenance : Change Console Port Speed

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.

18.3 Log and Trace

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

18.3.1 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:

Step 1. Type 24 in the main menu to display **Menu 24 – System Maintenance**.

Step 2. From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

```

Menu 24.3 - System Maintenance - Log and Trace

1. View Error Log

Please enter selection:

```

Figure 18-6 Menu 24.3 System Maintenance : Log and Trace

Step 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.

```

13 Sat Jan 1 00:00:00 2000 PP0d INFO LAN promiscuous mode <1>
14 Sat Jan 1 00:00:00 2000 PINI INFO Last errorlog repeat 1 Times
15 Sat Jan 1 00:00:00 2000 PINI INFO main: init completed
16 Sat Jan 1 00:00:02 2000 PP05 -WARN SNMP TRAP 3: link up
17 Sat Jan 1 00:00:02 2000 PP13 INFO sending request to NTP server(6)
20 Sat Jan 1 00:00:30 2000 PSSV -WARN SNMP TRAP 0: cold start

Clear Error Log (y/n):

```

Figure 18-7 Sample Error and Information Messages

18.4 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.

```
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
```

Figure 18-8 Menu 24.4 System Maintenance : Diagnostic

Follow the procedure next to get to display this menu:

- Step 1.** From the main menu, type 24 to open **Menu 24 – System Maintenance**.
- Step 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 18-3 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 19

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.

19.1 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 19-1 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.

19.2 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.

19.2.1 Backup Configuration Using FTP

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

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:

Figure 19-1 Menu 24.5 Backup Configuration

19.2.2 Using the FTP command from the DOS Prompt

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open” and the IP address of your ZyAIR.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter “root” and your SMT password as requested. The default is 1234.
- Step 5.** Enter “bin” to set transfer mode to binary.
- Step 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.
- Step 7.** Enter “quit” to exit the FTP prompt.

```

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

```

Figure 19-2 FTP Session Example

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

Table 19-2 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	<p>Anonymous.</p> <p>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.</p> <p>Normal.</p> <p>The server requires a unique User ID and Password to login.</p>
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.

Table 19-2 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

19.2.3 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:

- Step 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.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 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.
- Step 4.** Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.
- Step 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.

19.2.4 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 19-3 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.

19.3 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.

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:

Figure 19-3 Menu 24.6 Restore Configuration

19.4 Uploading Firmware and Configuration Files

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

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.

Menu 24.7 - System Maintenance - Upload Firmware

1. Upload System Firmware
2. Upload System Configuration File

Enter Menu Selection Number:

Figure 19-4 Menu 24.7 System Maintenance : Upload Firmware

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.

19.4.1 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.

```
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:
```

Figure 19-5 Menu 24.7.1 System Maintenance : Upload System Firmware

19.4.2 Configuration File Upload

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

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:

Figure 19-6 Menu 24.7.2 System Maintenance : Upload System Configuration File

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

19.4.3 Using the FTP command from the DOS Prompt Example

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter "open" and the IP address of your ZyAIR.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter "root" and your SMT password as requested. The default is 1234.
- Step 5.** Enter "bin" to set transfer mode to binary.
- Step 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.
- Step 7.** Enter "quit" to exit the FTP prompt.

```
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
```

Figure 19-7 FTP Session Example

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

19.4.4 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:

- Step 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.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 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.
- Step 4.** Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.
- Step 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.

19.4.5 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.

Chapter 20

System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

20.1 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.

```
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:
```

Figure 20-1 Menu 24 System Maintenance

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
B-3000> ?
Valid commands are:
sys          exit          device          ether
config       wlan          ip              ppp
bridge       hdap          radius          8021x
B-3000>
```

Figure 20-2 Valid CI Commands

20.2 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 and firewall logs.

- Step 1.** Select menu 24 in the main menu to open **Menu 24 – System Maintenance**.
- Step 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.

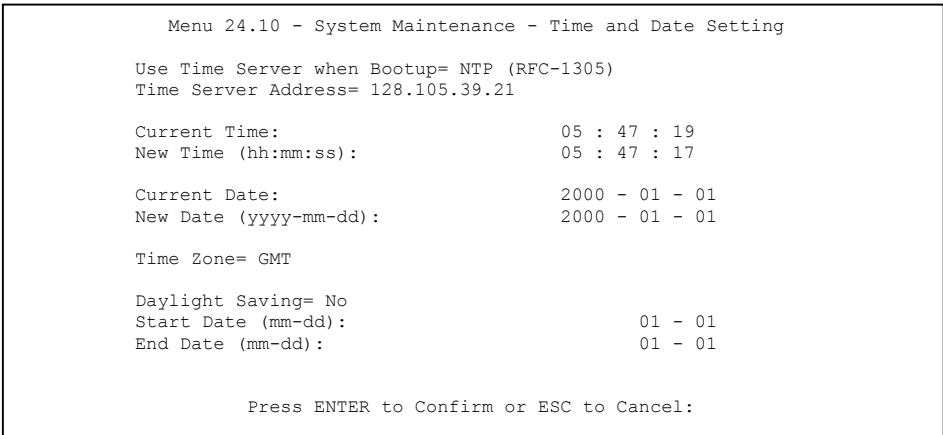


Figure 20-3 Menu 24.10 System Maintenance : Time and Date Setting

The following table describes the fields in this menu.

Table 20-1 Menu 24.10 System Maintenance : Time and Date Setting

FIELD	DESCRIPTION
Use Time Server when Bootup	<p>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.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868).</p> <p>None. The default, enter the time manually.</p>
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.
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.	

20.2.1 Resetting the Time

The ZyAIR resets the time in three instances:

- i. On leaving menu 24.10 after making changes.
- ii. When the ZyAIR starts up, if there is a time server configured in menu 24.10.
- iii. 24-hour intervals after starting.

Part VI:

APPENDICES

This part provides troubleshooting and background information about setting up your computer's IP address, wireless LAN, 802.1x, PPPoE, PPTP and IP subnetting. It also provides information on the antenna, PoE, command interpreter interface, NetBIOS commands and logs.

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

Chart A-1 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

Chart A-2 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.

Chart A-2 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I cannot ping any computer on the LAN.	<p>If the ETHN LED on the front panel is off, check the Ethernet cable connections between your ZyAIR and the Ethernet device.</p> <p>Check the Ethernet cable connections between the Ethernet device and the LAN computers.</p> <p>Check for faulty Ethernet cables.</p> <p>Make sure the LAN computer’s Ethernet adapter is installed and working properly.</p> <p>Verify that the IP address and the subnet mask of the ZyAIR, the Ethernet device and the LAN computers are on the same subnet.</p>

Problems with the Password

Chart A-3 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR.	<p>The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.</p> <p>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.</p>

Problems with Telnet

Chart A-4 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR through Telnet.	Refer to the <i>Problems with the Ethernet Interface</i> section for instructions on checking your Ethernet connection.

Problems with the WLAN Interface

Chart A-5 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

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 the Command Interpreter appendix for information on the command structure.

Chart B-1 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
<code>sys pwderrrtm</code>	This command displays the brute-force guessing password protection settings.
<code>sys pwderrrtm 0</code>	This command turns off the password's protection from brute-force guessing.
<code>sys pwderrrtm N</code>	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 pwderrrtm 5` This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

By default, the brute-force password guessing protection is turned ON with a 3-minute wait time.

Appendix C

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.

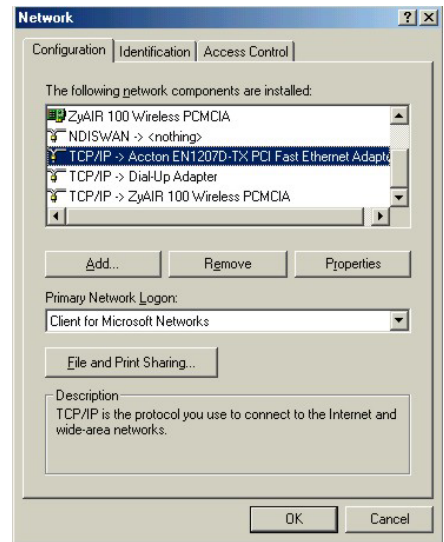
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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.



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:

- a. In the **Network** window, click **Add**.
- b. Select **Adapter** and then click **Add**.
- c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

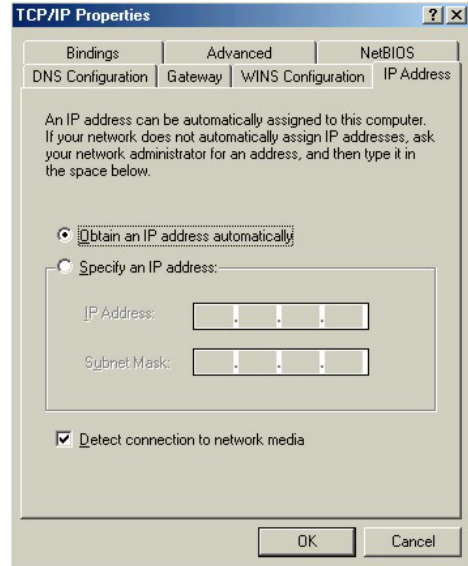
- a. In the **Network** window, click **Add**.
- b. Select **Protocol** and then click **Add**.
- c. Select **Microsoft** from the list of **manufacturers**.
- d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

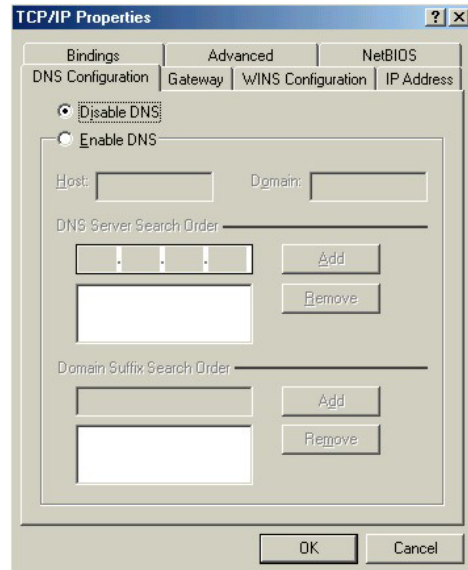
- a. Click **Add**.
- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

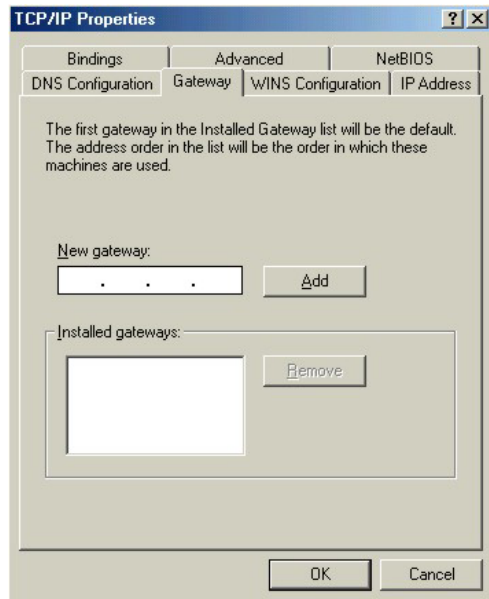
1. Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



2. 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).



3. 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**.



4. Click **OK** to save and close the **TCP/IP Properties** window.
5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
6. Turn on your ZyAIR and restart your computer when prompted.

Verifying Your Computer's IP Address

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

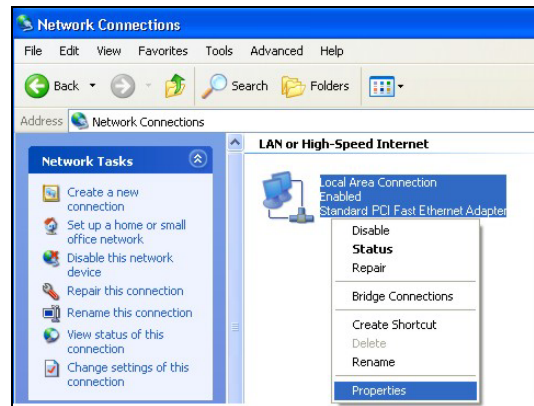
1. For Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.



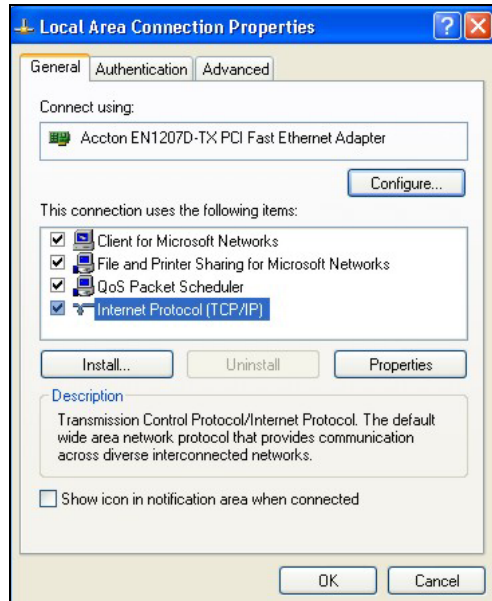
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



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



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

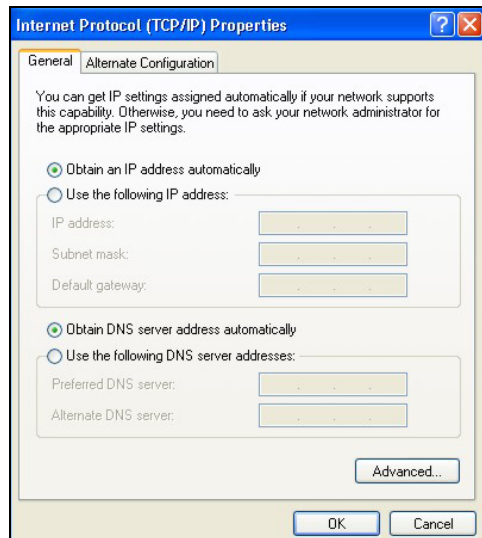


5. The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

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

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

Click **Advanced**.



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

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

-In the **IP Settings** tab, in IP addresses, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

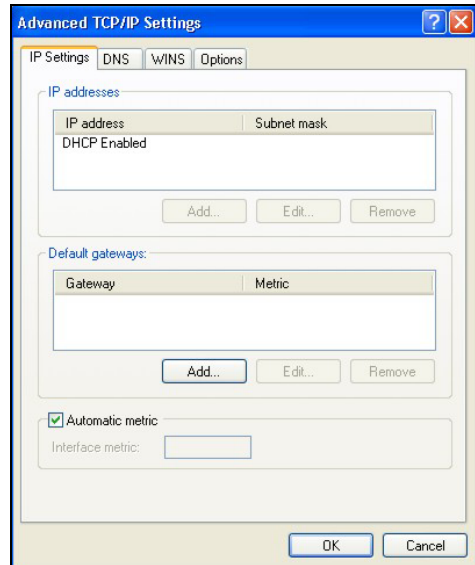
-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

-Click **OK** when finished.

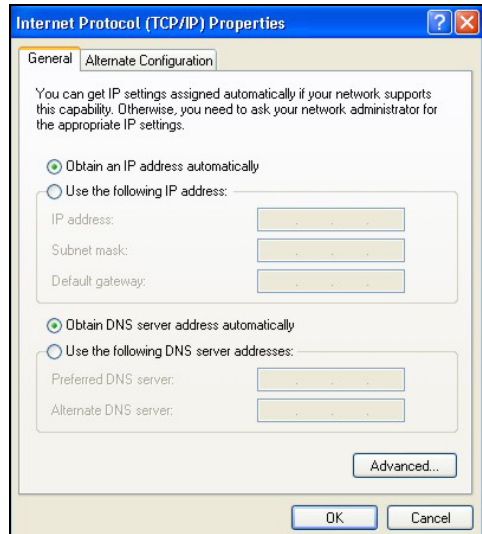


7. In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

-Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

-If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

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



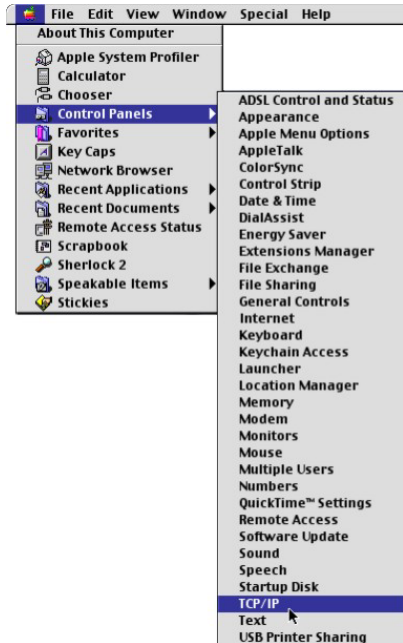
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

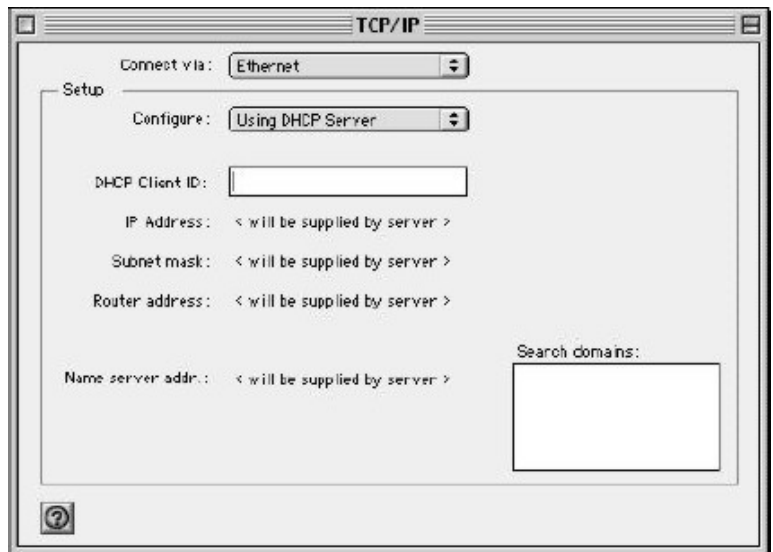
1. Click **Start, All Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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



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



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

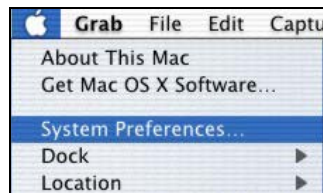
4. For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your ZyAIR in the **Router address** box.
5. Close the **TCP/IP 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 Your Computer's IP Address

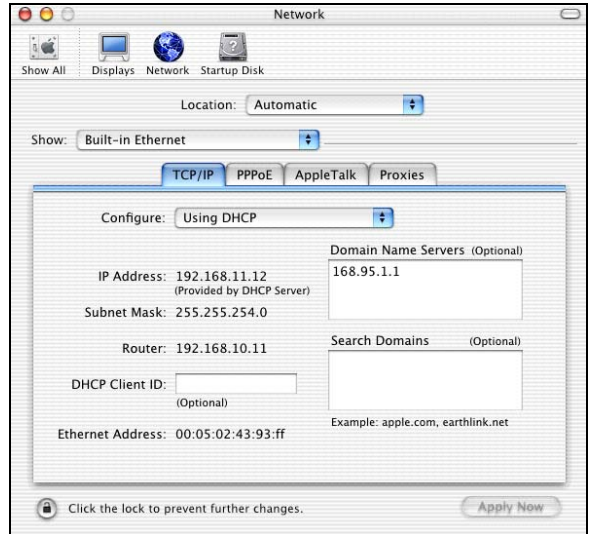
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

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



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.
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 Your Computer's IP Address

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

Appendix D

Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area. WLAN is not available on all models.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

1. It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.
4. It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".
5. It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits. On September 16, 1999, the 802.11b provided much higher data rates of up to 11Mbps, while maintaining the 802.11 protocol.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence

Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. 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). See the following diagram of an example of an Ad-hoc wireless LAN.

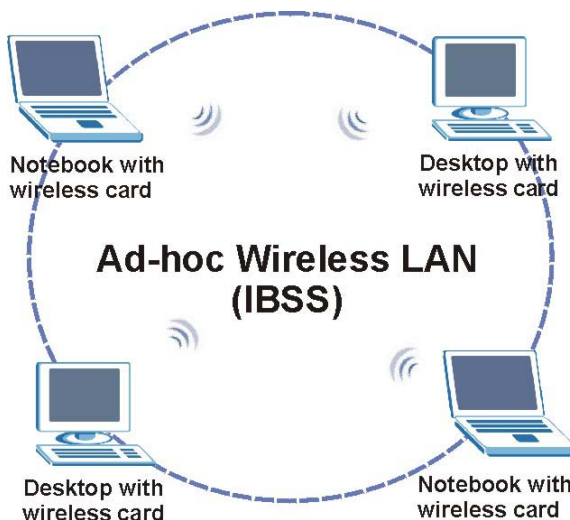


Diagram D-1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access

points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between access points and seamless campus-wide coverage is possible.

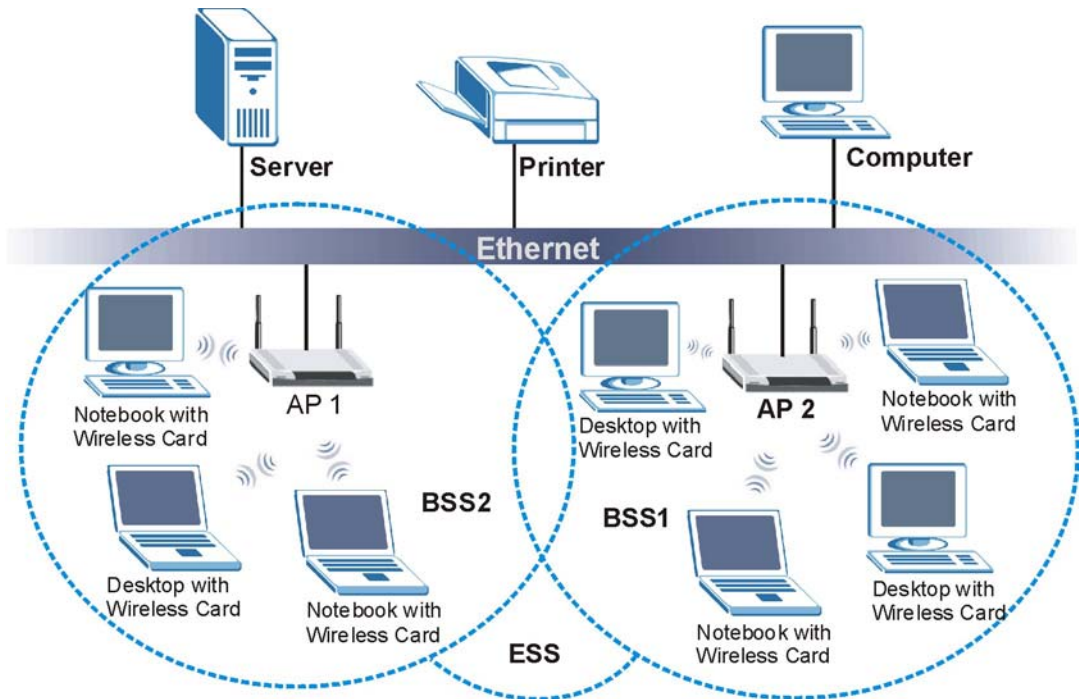


Diagram D-2 ESS Provides Campus-Wide Coverage

Appendix E

Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

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.

Advantages of the IEEE 802.1x

- 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 Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

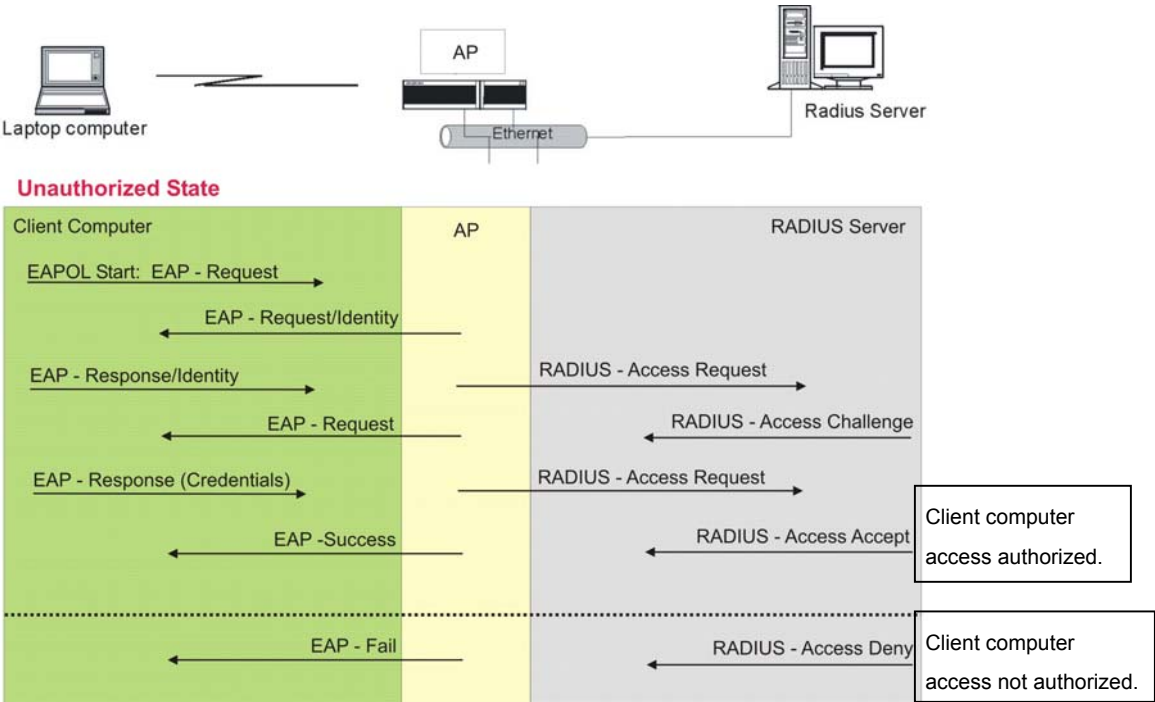


Diagram E-1 Sequences for EAP MD5–Challenge Authentication

Appendix F

Types of EAP Authentication

This appendix discusses the four popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS** and **PEAP**. 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 and EAP-MSCHAPv2, for client authentication.

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, simple user name and password pair is more practical. The following table is a comparison of the features of four authentication types.

Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP
Mutual Authentication	No	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional
Certificate – Server	No	Yes	Yes	Yes
Dynamic Key Exchange	No	Yes	Yes	Yes
Credential Security	None	Strong	Strong	Strong
Deployment Difficulty	Easy	Hard	Moderate	Moderate
Wireless Security	Poor	Best	Good	Good
Client Identity Protection	No	No	Yes	Yes

Appendix G

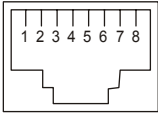
Power over Ethernet Specifications

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

Chart 1 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Chart G-2 Power over Ethernet Injector RJ-45 Port Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

Appendix H

Antenna Selection and Positioning Recommendation

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.

Choosing the right antennas and positioning them 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. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The 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 transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend 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.

Connector Type

The ZyAIR is equipped with a reverse polarity SMA jack, so it will work with any 2.4GHz wireless antenna with a reverse polarity SMA plug.

Appendix I

PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit), which connects to a DSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN & ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

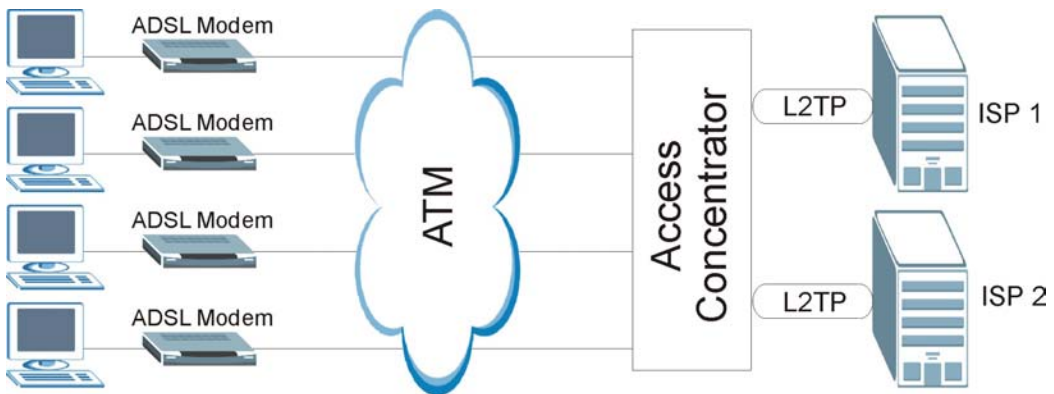


Diagram I-1 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

ZyAIR as a PPPoE Client

When using the ZyAIR as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

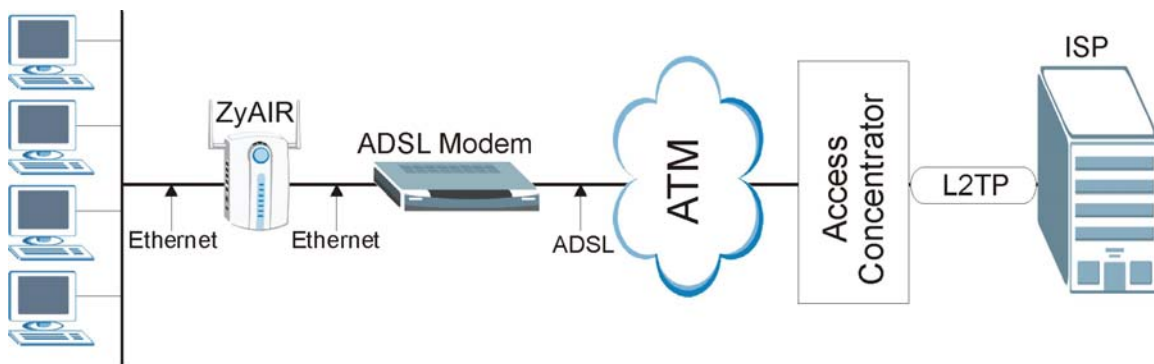


Diagram I-2 ZyAIR as a PPPoE Client

Appendix J

PPTP

What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

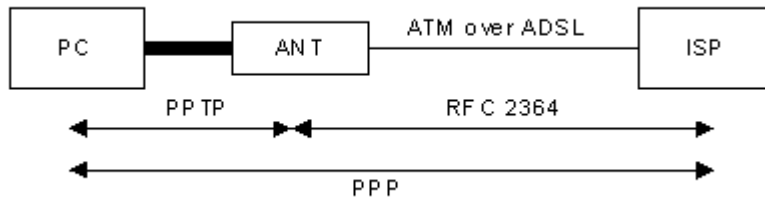


Diagram J-1 Transport PPP frames over Ethernet

PPTP and the ZyAIR

When the ZyAIR is deployed in such a setup, it appears as a PC to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the ZyAIR's Internet connection. In NAT mode, the ZyAIR is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The ZyAIR initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco’s Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

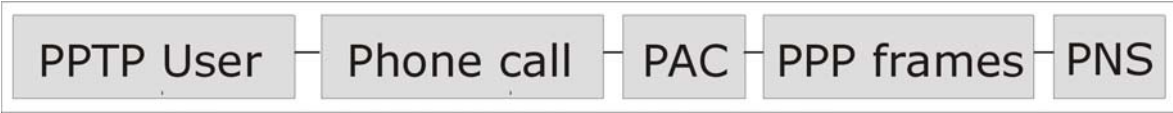


Diagram J-2 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft’s implementation, the PC, and hence the ZyAIR, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

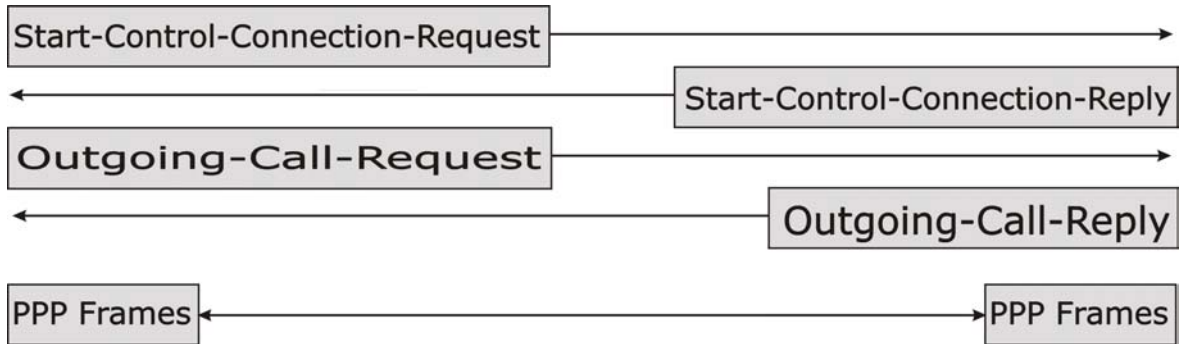


Diagram J-3 Example Message Exchange between PC and an ANT

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the **Call ID** field in the GRE header.

Appendix K

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.)

Chart K-1 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

Host IDs of all zeros or all ones are not allowed.

Therefore:

- A class “C” network (8 host bits) can have $2^8 - 2$ or 254 hosts.
- A class “B” address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class “A” address (24 host bits) can have $2^{24} - 2$ hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Chart K-2 Allowed IP Address Range By Class

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

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

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

Chart K-3 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

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

sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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

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

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

Chart K-4 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.

	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.

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

Chart K-5 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

Chart K-6 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 (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart K-7 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0		Lowest Host ID: 192.168.1.1
Broadcast Address: 192.168.1.63		Highest Host ID: 192.168.1.62

Chart K-8 Subnet 2

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

Chart K-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000

Chart K-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128		Lowest Host ID: 192.168.1.129
Broadcast Address: 192.168.1.191		Highest Host ID: 192.168.1.190

Chart K-10 Subnet 4

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

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

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

Chart K-11 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	223	254	255

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

Chart K-12 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 *Chart J-1*) available for subnetting.

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

Chart K-13 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

Chart K-13 Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 L

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.

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 M

NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See the *Command Interpreter* appendix for information on the command structure.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to do the following :

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN.
- Allow or disallow the sending of NetBIOS packets from the WAN to the LAN.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for a ZyAIR

```
===== NetBIOS Filter Status =====
      LAN to WAN:           Forward
      WAN to LAN:           Forward
      IPsec Packets:         Forward
      Trigger Dial:         Disabled
```

Diagram M-1 NetBIOS Display Filter Settings Command Without DMZ Example

The filter types and their default settings are as follows.

Chart M-1 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
LAN to WAN	This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the WAN.	Forward

Chart M-1 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
WAN to LAN	This field displays whether NetBIOS packets are blocked or forwarded from the WAN to the LAN.	Forward
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

Syntax: `sys filter netbios config <type>`

Usage = `config:`

`0 = LAN to WAN`

`1 = WAN to LAN`

`6 = IPSec packet pass through`

`7 = Trigger Dial`

Example commands

Command: `sys filter netbios config 0 on`

This command blocks LAN to WAN NetBIOS packets

Command: `sys filter netbios config 1 off`

This command forwards WAN to LAN NetBIOS packets

Command: `sys filter netbios config 6 on`

This command blocks IPSec NetBIOS packets

Command: `sys filter netbios config 7 off`

This command stops NetBIOS commands from initiating calls.

Appendix N

Log Descriptions

Chart N-1 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

Chart N-2 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.

Chart N-2 System Maintenance Logs

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.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.

Chart N-3 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
	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

Chart N-3 ICMP Notes

TYPE	CODE	DESCRIPTION
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

Chart N-4 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

Chart N-5 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 O

Power Adaptor Specifications

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)
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)
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)
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)

JAPAN PLUG STANDARDS

AC Power Adaptor Model	JOD-48-1124
Input Power	AC100Volts/ 50/60Hz/ 27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	T-Mark (Japan Dentori)

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)

Appendix P

Index

A

Address Assignment.....	3-5, 8-1
Ad-hoc Configuration.....	D-2
Alternative Subnet Mask Notation	K-3
Antenna	
Directional	G-2
Omni-directional	G-1
Types.....	G-1
Antenna gain	G-1
Applications	1-6
auto-negotiation.....	1-2

B

backup	19-2
Backup.....	10-9
Basic Service Set.....	D-2
BSS.....	<i>See</i> Basic Service Set

C

CA	F-1
Certificate Authority.....	<i>See</i> CA
Channel ID	5-6, 13-3
Classes of IP Addresses.....	K-1
Collision	18-2
Command Interpreter	20-1
Community.....	16-2
Computer's IP Address	C-1
Copyright.....	ii
CPU Load.....	18-3
Customer Support.....	v

D

Data encryption	3-1
Default.....	10-12
DHCP	18-4

Diagnostic.....	18-6
Diagnostic Tools.....	18-1
Direct Sequence Spread Spectrum.....	D-2
Distribution System	D-3
DS	<i>See</i> Distribution System
DSSS	<i>See</i> Direct Sequence Spread Spectrum

E

EAP	1-5
EAP Authentication	F-1
MD5	F-1
TLS.....	F-1
TTLS.....	F-1
Encapsulation	
PPP over Ethernet.....	H-1
Error Log	18-5
Error/Information Messages	
Sample.....	18-5
ESS ..	<i>See</i> Extended Service Set. <i>See</i> Extended Service Set
ESS ID	3-1
Extended Service Set	D-3, 5-2
Extended Service Set IDentification	5-6

F

FCC	iii
FHSS	<i>See</i> Frequency-Hopping Spread Spectrum
Filename Conventions	19-1
Firmware File	
Maintenance	10-7, 10-9
Fragment Threshold.....	13-3
Fragmentation Threshold.....	5-4
Frequency-Hopping Spread Spectrum	D-2
FTP File Transfer.....	19-7

G

General Setup	3-2, 4-1, 12-1
---------------------	----------------

H

Hidden Menus.....	11-4
Host	4-3
Host IDs.....	K-1

I

IBSS.....	<i>See</i> Independent Basic Service Set
IEEE 802.11	D-1
Deployment Issues	E-1
Security Flaws.....	E-1
IEEE 802.1x	E-1, 1-5
Advantages.....	E-1
Independent Basic Service Set.....	D-2, 5-1, 10-6
Infrastructure Configuration	D-3
Internet access.....	13-1
Internet Access	1-7
Internet Security Gateway	1-1
IP Address	3-5, 3-6, 8-1, 8-2, 13-2, 18-4, 18-6
IP Addressing	K-1
IP Classes.....	K-1

L

Link type.....	18-2
Log and Trace.....	18-5
Log Descriptions.....	N-1
Logs	9-1

M

MAC Address Filter Action.....	6-7, 13-6
MAC Address Filtering	13-5
Main Menu	11-4
Management Information Base (MIB).....	16-2
MD5.....	F-1
Message Digest Algorithm 5	<i>See</i> MD5
Multicast.....	7-1

N

NAT.....	3-6
Network Management	1-5
Network Topology With RADIUS Server Example.....	E-2

P

Packets	18-2
Password	4-2, 11-1, 16-2
Ping	18-6
PPTP	I-1
Private IP Address.....	3-5, 8-1

Q

Quick Start Guide.....	xvii, 2-1
------------------------	-----------

R

RADIUS.....	1-5
RAS.....	18-4
Rate	
Receiving.....	18-2
Transmission.....	18-2
Related Documentation.....	xvii
Remote Authentication Dial In User Service	<i>See</i> RADIUS
Remote Node	18-2
Required fields	11-4
Restore	10-10
Restore Configuration	19-5
RF signals	D-2
Roaming	
Example.....	5-10
Requirements	5-11
RTS Threshold	5-3, 13-3

S

Server	4-5
Service	iv
Service Set	5-6
SMT Menu Overview	11-2
SNMP	
Community	16-3
Configuration.....	16-2
Get	16-2
GetNext	16-2
Manager.....	16-2
MIBs	16-2
Set.....	16-2

Trap.....	16-2
Traps	16-3, 16-4
Trusted Host.....	16-3
Subnet Mask.....	3-6, 8-1, 13-2, 18-4
Subnet Masks	K-2
Subnetting	K-3
Supporting Disk.....	xvii
System	
Console Port Speed.....	18-4
Diagnostic	18-5
Log and Trace.....	18-5
System Information.....	18-3
System Status.....	18-1
Time and Date.....	20-2
System Information	18-3
System Information & Diagnosis	18-1
System Maintenance.....	18-1, 18-3, 19-2, 19-4, 19-5, 19-6, 19-9, 20-1, 20-2, 20-3
System Management Terminal.....	11-4
System Name.....	4-2
System Status	18-2

T

TCP/IP.....	18-6
TFTP File Transfer	19-9
Time and Date Setting	20-2
Time Server.....	20-3
Time Zone	20-3
TLS.....	F-1
Trace Records.....	18-5
Transport Layer Security	See TLS
Troubleshooting	
Accessing ZyAIR.....	A-2, A-3

Ethernet Port.....	A-1
Password	A-2
Start-Up.....	A-1
TTLS.....	F-1
Tunneled Transport Layer Service.....	See TTLS

U

Upload Firmware	19-6
User Profiles	6-10, 14-1

V

Valid CI Commands	20-1
-------------------------	------

W

Web Configurator	2-1, 2-3
WEP.....	3-1
WEP Encryption.....	6-4, 13-4
Wireless LAN	D-1, 13-2
Benefits	D-1
Wireless LAN Setup	13-2
Wizard Setup	3-1, 3-2, 3-3, 3-5
WLAN	See Wireless LAN

Z

ZyNOS.....	19-1, 19-2
ZyNOS F/W Version	19-1
ZyXEL Limited Warranty	
Note.....	iv