

# ***ZyAIR G-500***

***802.11g Wireless Access Point***

## ***User's Guide***

Version 3.50

April 2004



# Copyright

## **Copyright © 2004 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.

## Caution

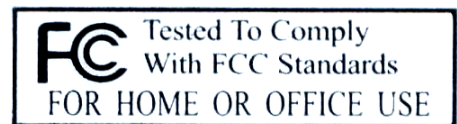
1. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## 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

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



# 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	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE <sup>1</sup> FAX <sup>1</sup>	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	<a href="mailto:support@zyxel.com.tw">support@zyxel.com.tw</a>  <a href="mailto:sales@zyxel.com.tw">sales@zyxel.com.tw</a>	+886-3-578-3942  +886-3-578-2439	<a href="http://www.zyxel.com">www.zyxel.com</a> <a href="http://www.europe.zyxel.com">www.europe.zyxel.com</a> <a href="ftp://ftp.zyxel.com">ftp.zyxel.com</a> <a href="ftp://ftp.europe.zyxel.com">ftp.europe.zyxel.com</a>	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	<a href="mailto:support@zyxel.com">support@zyxel.com</a>  <a href="mailto:sales@zyxel.com">sales@zyxel.com</a>	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	<a href="http://www.us.zyxel.com">www.us.zyxel.com</a>  <a href="ftp://ftp.us.zyxel.com">ftp.us.zyxel.com</a>	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	<a href="mailto:support@zyxel.de">support@zyxel.de</a>  <a href="mailto:sales@zyxel.de">sales@zyxel.de</a>	+49-2405-6909-0  +49-2405-6909-99	<a href="http://www.zyxel.de">www.zyxel.de</a>	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	<a href="mailto:info@zyxel.fr">info@zyxel.fr</a>	+33 (0)4 72 52 97 97  +33 (0)4 72 52 19 20	<a href="http://www.zyxel.fr">www.zyxel.fr</a>	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	<a href="mailto:support@zyxel.es">support@zyxel.es</a>  <a href="mailto:sales@zyxel.es">sales@zyxel.es</a>	+34 902 195 420  +34 913 005 345	<a href="http://www.zyxel.es">www.zyxel.es</a>	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	<a href="mailto:support@zyxel.dk">support@zyxel.dk</a>  <a href="mailto:sales@zyxel.dk">sales@zyxel.dk</a>	+45 39 55 07 00  +45 39 55 07 07	<a href="http://www.zyxel.dk">www.zyxel.dk</a>	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	<a href="mailto:support@zyxel.no">support@zyxel.no</a>  <a href="mailto:sales@zyxel.no">sales@zyxel.no</a>	+47 22 80 61 80  +47 22 80 61 81	<a href="http://www.zyxel.no">www.zyxel.no</a>	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SWEDEN	<a href="mailto:support@zyxel.se">support@zyxel.se</a>  <a href="mailto:sales@zyxel.se">sales@zyxel.se</a>	+46 31 744 7700  +46 31 744 7701	<a href="http://www.zyxel.se">www.zyxel.se</a>	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden

<sup>1</sup> “+” is the (prefix) number you enter to make an international telephone call.

## ZyAIR G-500 Wireless Access Point User's Guide

---

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE <sup>1</sup> FAX <sup>1</sup>	WEB SITE FTP SITE	REGULAR MAIL
FINLAND	<a href="mailto:support@zyxel.fi">support@zyxel.fi</a> <a href="mailto:sales@zyxel.fi">sales@zyxel.fi</a>	+358-9-4780-8411 +358-9-4780 8448	<a href="http://www.zyxel.fi">www.zyxel.fi</a>	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

# Table of Contents

Copyright.....	ii
Federal Communications Commission (FCC) Interference Statement.....	iii
ZyXEL Limited Warranty.....	iv
Customer Support.....	v
List of Figures.....	xii
List of Tables.....	xv
Preface.....	xvii
<b>OVERVIEW.....</b>	<b>I</b>
<b>Chapter 1 Getting to Know Your ZyAIR.....</b>	<b>1-1</b>
1.1 Introducing the ZyAIR Wireless Access Point.....	1-1
1.2 ZyAIR Features.....	1-1
1.3 Applications for the ZyAIR.....	1-3
1.3.1 Internet Access Application.....	1-4
1.3.2 Corporation Network Application.....	1-4
<b>Chapter 2 Introducing the Web Configurator.....</b>	<b>2-1</b>
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
<b>Chapter 3 Wizard Setup.....</b>	<b>3-1</b>
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.....	3-4
3.4.1 IP Address Assignment.....	3-4
3.4.2 IP Address and Subnet Mask.....	3-5
3.5 Basic Setup Complete.....	3-7
<b>SYSTEM, WIRELESS AND IP.....</b>	<b>III</b>
<b>Chapter 4 System Screens.....</b>	<b>4-1</b>
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
<b>Chapter 5 Wireless Configuration and Roaming.....</b>	<b>5-1</b>
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 Roaming.....	5-6
5.4.1	Requirements for Roaming.....	5-8
<b>Chapter 6</b>	<b>Wireless Security.....</b>	<b>6-1</b>
6.1	Wireless Security Overview.....	6-1
6.2	WEP Overview.....	6-1
6.2.1	Data Encryption.....	6-2
6.2.2	Authentication.....	6-2
6.3	Preamble Type.....	6-3
6.4	Configuring WEP Encryption.....	6-3
6.5	MAC Filter.....	6-6
6.6	802.1x Overview.....	6-8
6.7	Introduction to RADIUS.....	6-8
6.7.1	EAP Authentication Overview.....	6-9
6.8	Dynamic WEP Key Exchange.....	6-10
6.9	Introduction to WPA.....	6-11
6.9.1	User Authentication.....	6-11
6.9.2	Encryption.....	6-11
6.10	WPA-PSK Application Example.....	6-12
6.11	WPA with RADIUS Application Example.....	6-12
6.12	Security Parameters Summary.....	6-13
6.13	Wireless Client WPA Supplicants.....	6-14
6.14	Configuring 802.1x and WPA.....	6-14
6.14.1	Authentication Required: 802.1x.....	6-15
6.14.2	Authentication Required: WPA.....	6-18
6.14.3	Authentication Required: WPA-PSK.....	6-20
6.15	Introduction to Local User Database.....	6-21
6.16	Configuring Local User Database.....	6-21
6.17	Configuring RADIUS.....	6-23
<b>Chapter 7</b>	<b>IP Screen.....</b>	<b>7-1</b>
7.1	Factory Ethernet Defaults.....	7-1
7.2	TCP/IP Parameters.....	7-1
7.2.1	IP Address and Subnet Mask.....	7-1
7.3	Configuring IP.....	7-1
<b>REMOTE MANAGEMENT AND LOGS.....</b>		<b>IV</b>
<b>Chapter 8</b>	<b>Remote Management.....</b>	<b>8-1</b>



8.1	Remote Management Overview .....	8-1
8.1.1	Remote Management Limitations .....	8-1
8.1.2	System Timeout .....	8-1
8.2	Telnet .....	8-2
8.3	Configuring TELNET .....	8-2
8.4	Configuring FTP .....	8-3
8.5	Configuring WWW .....	8-4
8.6	Configuring SNMP .....	8-5
8.6.1	Supported MIBs .....	8-7
8.6.2	SNMP Traps .....	8-7
8.6.3	REMOTE MANAGEMENT: SNMP .....	8-7
<b>Chapter 9</b>	<b>Logs Screens .....</b>	<b>9-1</b>
9.1	Configuring View Log .....	9-1
9.2	Configuring Log Settings .....	9-2
<b>MAINTENANCE</b>	<b>.....</b>	<b>V</b>
<b>Chapter 10</b>	<b>Maintenance .....</b>	<b>10-1</b>
10.1	Maintenance Overview .....	10-1
10.2	System Status Screen .....	10-1
10.2.1	System Statistics .....	10-2
10.3	Association List .....	10-3
10.4	F/W Upload Screen .....	10-4
10.5	Configuration Screen .....	10-7
10.5.1	Backup Configuration .....	10-8
10.5.2	Restore Configuration .....	10-9
10.5.3	Back to Factory Defaults .....	10-10
10.6	Restart Screen .....	10-11
<b>SMT CONFIGURATION</b>	<b>.....</b>	<b>V</b>
<b>Chapter 11</b>	<b>Introducing the SMT .....</b>	<b>11-1</b>
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
<b>Chapter 12</b>	<b>General Setup .....</b>	<b>12-1</b>
12.1	General Setup .....	12-1
12.1.1	Procedure To Configure Menu 1 .....	12-1
<b>Chapter 13</b>	<b>LAN Setup .....</b>	<b>13-1</b>
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
<b>Chapter 14</b>	<b>Dial-in User Setup .....</b>	<b>14-1</b>
14.1	Dial-in User Setup .....	14-1
<b>Chapter 15</b>	<b>SNMP Configuration .....</b>	<b>15-1</b>
15.1	About SNMP .....	15-1
15.2	Supported MIBs .....	15-2
15.3	SNMP Configuration .....	15-2
15.4	SNMP Traps .....	15-3
<b>Chapter 16</b>	<b>System Security .....</b>	<b>16-1</b>
16.1	System Security .....	16-1
16.1.1	System Password .....	16-1
16.1.2	Configuring External RADIUS Server .....	16-1
16.1.3	802.1x .....	16-3
<b>Chapter 17</b>	<b>System Information and Diagnosis.....</b>	<b>17-1</b>
17.1	Overview.....	17-1
17.2	System Status.....	17-1
17.3	System Information.....	17-3
17.3.1	System Information.....	17-3
17.3.2	Console Port Speed.....	17-4
17.4	Log and Trace .....	17-5
17.4.1	Viewing Error Log.....	17-5
17.5	Diagnostic .....	17-6
<b>Chapter 18</b>	<b>Firmware and Configuration File Maintenance .....</b>	<b>18-1</b>
18.1	Filename Conventions .....	18-1
18.2	Backup Configuration.....	18-2
18.2.1	Backup Configuration Using FTP.....	18-2
18.2.2	Using the FTP command from the DOS Prompt .....	18-3
18.2.3	Backup Configuration Using TFTP .....	18-4
18.2.4	Example: TFTP Command .....	18-4
18.3	Restore Configuration.....	18-5
18.4	Uploading Firmware and Configuration Files .....	18-6
18.4.1	Firmware Upload .....	18-7
18.4.2	Configuration File Upload .....	18-7
18.4.3	Using the FTP command from the DOS Prompt Example .....	18-8
18.4.4	TFTP File Upload .....	18-9
18.4.5	Example: TFTP Command .....	18-10
<b>Chapter 19</b>	<b>System Maintenance and Information.....</b>	<b>19-1</b>
19.1	Command Interpreter Mode.....	19-1
19.2	Time and Date Setting .....	19-2
19.2.1	Resetting the Time .....	19-3
<b>Chapter 20</b>	<b>Remote Management.....</b>	<b>20-1</b>

---

20.1	Telnet .....	20-1
20.2	FTP.....	20-1
20.3	Web .....	20-1
20.4	Remote Management .....	20-1
20.4.1	Remote Management Setup.....	20-2
20.4.2	Remote Management Limitations .....	20-3
20.5	System Timeout .....	20-3
<b>APPENDICES</b>	.....	<b>VII</b>
<b>Appendix A Troubleshooting</b>	.....	<b>A-1</b>
<b>Appendix B Brute-Force Password Guessing Protection</b>	.....	<b>B-1</b>
<b>Appendix C Setting up Your Computer's IP Address</b>	.....	<b>C-1</b>
<b>Appendix D Wireless LAN and IEEE 802.11</b>	.....	<b>D-1</b>
<b>Appendix E Wireless LAN With IEEE 802.1x</b>	.....	<b>E-1</b>
<b>Appendix F Types of EAP Authentication</b>	.....	<b>F-1</b>
<b>Appendix G IP Subnetting</b>	.....	<b>G-1</b>
<b>Appendix H Command Interpreter</b>	.....	<b>H-1</b>
<b>Appendix I Log Descriptions</b>	.....	<b>I-1</b>
<b>Appendix J Index</b>	.....	<b>J-1</b>

# List of Figures

Figure 1-1 Internet Access Application.....	1-4
Figure 1-2 Corporation Network Application.....	1-5
Figure 2-1 Change Password Screen.....	2-1
Figure 2-2 Navigating the ZyAIR Web Configurator.....	2-3
Figure 3-1 Wizard 1 : General Setup.....	3-2
Figure 3-2 Wizard 2 : Wireless LAN Setup.....	3-3
Figure 3-3 Wizard 3 : IP Address Assignment.....	3-6
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 Roaming Example.....	5-7
Figure 5-7 Roaming.....	5-8
Figure 6-1 ZyAIR Wireless Security Levels.....	6-1
Figure 6-2 WEP Authentication Steps.....	6-2
Figure 6-3 Wireless.....	6-4
Figure 6-4 MAC Address Filter.....	6-7
Figure 6-5 EAP Authentication.....	6-10
Figure 6-6 WPA - PSK Authentication.....	6-12
Figure 6-7 WPA with RADIUS Application Example.....	6-13
Figure 6-8 Wireless LAN: 802.1x/WPA.....	6-15
Figure 6-9 Wireless LAN: 802.1x/WPA for 802.1x Protocol.....	6-16
Figure 6-10 Wireless LAN: 802.1x/WPA for WPA Protocol.....	6-19
Figure 6-11 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol.....	6-20
Figure 6-12 Local User Database.....	6-22
Figure 6-13 RADIUS.....	6-23
Figure 7-1 IP Setup.....	7-1
Figure 8-1 Telnet Configuration on a TCP/IP Network.....	8-2
Figure 8-2 Telnet.....	8-2
Figure 8-3 FTP.....	8-3
Figure 8-4 WWW.....	8-4
Figure 8-5 SNMP Management Model.....	8-6
Figure 8-6 SNMP.....	8-8
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 Firmware Upload.....	10-5
Figure 10-5 Firmware Upload In Process .....	10-6
Figure 10-6 Network Temporarily Disconnected.....	10-6
Figure 10-7 Firmware Upload Error .....	10-7
Figure 10-8 Configuration .....	10-8
Figure 10-9 Configuration Upload Successful.....	10-9
Figure 10-10 Network Temporarily Disconnected.....	10-10
Figure 10-11 Configuration Upload Error.....	10-10
Figure 10-12 Reset Warning Message.....	10-11
Figure 10-13 Restart Screen.....	10-11
Figure 11-1 Login Screen.....	11-1
Figure 11-2 Menu 23.1 System Security : Change Password .....	11-2
Figure 11-3 ZyAIR G-500 SMT Menu Overview Example .....	11-3
Figure 11-4 ZyAIR G-500 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.....	13-6
Figure 13-5 Menu 3.5.1 WLAN MAC Address Filter .....	13-6
Figure 13-6 Menu 3.5 Wireless LAN Setup.....	13-8
Figure 13-7 Menu 3.5.2 Roaming Configuration.....	13-8
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 SNMP Management Model.....	15-1
Figure 15-2 Menu 22 SNMP Configuration.....	15-3
Figure 16-1 Menu 23 System Security.....	16-1
Figure 16-2 Menu 23 System Security.....	16-1
Figure 16-3 Menu 23.2 System Security : RADIUS Server .....	16-2
Figure 16-4 Menu 23 System Security.....	16-3
Figure 16-5 Menu 23.4 System Security : IEEE802.1x .....	16-4
Figure 17-1 Menu 24 System Maintenance .....	17-1
Figure 17-2 Menu 24.1 System Maintenance : Status.....	17-2
Figure 17-3 Menu 24.2 System Information and Console Port Speed.....	17-3
Figure 17-4 Menu 24.2.1 System Information : Information.....	17-3
Figure 17-5 Menu 24.2.2 System Maintenance : Change Console Port Speed.....	17-4
Figure 17-6 Menu 24.3 System Maintenance : Log and Trace .....	17-5
Figure 17-7 Sample Error and Information Messages .....	17-5

Figure 17-8 Menu 24.4 System Maintenance : Diagnostic .....	17-6
Figure 18-1 Menu 24.5 Backup Configuration .....	18-2
Figure 18-2 FTP Session Example.....	18-3
Figure 18-3 Menu 24.6 Restore Configuration .....	18-6
Figure 18-4 Menu 24.7 System Maintenance : Upload Firmware .....	18-6
Figure 18-5 Menu 24.7.1 System Maintenance : Upload System Firmware .....	18-7
Figure 18-6 Menu 24.7.2 System Maintenance : Upload System Configuration File .....	18-8
Figure 18-7 FTP Session Example.....	18-9
Figure 19-1 Menu 24 System Maintenance .....	19-1
Figure 19-2 Valid CI Commands .....	19-1
Figure 19-3 Menu 24.10 System Maintenance : Time and Date Setting .....	19-2
Figure 20-1 Telnet Configuration on a TCP/IP Network .....	20-1
Figure 20-2 Menu 24.11 Remote Management Control .....	20-2

# List of Tables

Table 3-1 Wizard 1 : General Setup .....	3-2
Table 3-2 Wizard 2 : Wireless LAN Setup .....	3-3
Table 3-3 Private IP Address Ranges .....	3-5
Table 3-4 Wizard 3 : IP Address Assignment .....	3-6
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 Roaming .....	5-9
Table 6-1 Wireless .....	6-4
Table 6-2 MAC Address Filter .....	6-8
Table 6-3 Wireless Security Relational Matrix .....	6-13
Table 6-4 Wireless LAN: 802.1x/WPA .....	6-15
Table 6-5 Wireless LAN: 802.1x/WPA for 802.1x Protocol .....	6-16
Table 6-6 Wireless LAN: 802.1x/WPA for WPA Protocol .....	6-19
Table 6-7 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol .....	6-21
Table 6-8 Local User Database .....	6-23
Table 6-9 RADIUS .....	6-24
Table 7-1 IP Setup .....	7-2
Table 8-1 Telnet .....	8-2
Table 8-2 FTP .....	8-4
Table 8-3 WWW .....	8-5
Table 8-4 SNMP Traps .....	8-7
Table 8-5 Ports and Interface Types .....	8-7
Table 8-6 SNMP .....	8-8
Table 9-1 View Log .....	9-2
Table 9-2 Log Settings .....	9-4
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 Firmware Upload .....	10-5
Table 10-5 Restore Configuration .....	10-9
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 .....	13-7
Table 13-4 Menu 3.5.2 Roaming Configuration .....	13-8

Table 14-1 Menu 14.1- Edit Dial-in User .....	14-2
Table 15-1 Menu 22 SNMP Configuration .....	15-3
Table 15-2 SNMP Traps.....	15-4
Table 16-1 Menu 23.2 System Security : RADIUS Server.....	16-2
Table 16-2 Menu 23.4 System Security : IEEE802.1x .....	16-4
Table 17-1 Menu 24.1 System Maintenance : Status .....	17-2
Table 17-2 Menu 24.2.1 System Maintenance : Information.....	17-4
Table 17-3 Menu 24.4 System Maintenance Menu : Diagnostic .....	17-6
Table 18-1 Filename Conventions .....	18-2
Table 18-2 General Commands for Third Party FTP Clients.....	18-3
Table 18-3 General Commands for Third Party TFTP Clients .....	18-5
Table 19-1 Menu 24.10 System Maintenance : Time and Date Setting .....	19-3
Table 20-1 Menu 24.11 Remote Management Control.....	20-2



# Preface

Congratulations on your purchase from the ZyAIR G-500 802.11g Wireless Access Point.

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

This User's Guide is designed to guide you through the configuration of your 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 solely on features not configurable by the web configurator.

**Don't forget to register your product online for free future product updates and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.**

## 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](http://www.zyxel.com) contains additional support documentation. Please also refer to [www.zyxel.com](http://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 G-500 802.11g Wireless Access Point 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](mailto:techwriters@zyxel.com.tw) or send regular mail to The Technical Writing Team, ZyxEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

---

# 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 setup the ZyAIR.



# Chapter 1

## Getting to Know Your ZyAIR

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

### 1.1 Introducing the ZyAIR Wireless Access Point

The ZyAIR 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, WPA (Wi-Fi Protected Access) and MAC address filtering. Both IEEE802.11b and IEEE802.11g compliant WLAN devices can associate with the ZyAIR.

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.

#### **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.

## 802.11g Wireless LAN Standard

ZyAIR products containing the letter “G” in the model name, such as ZyAIR G-500 and ZyAIR G-2000, comply with the 802.11g wireless standard.

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

IEEE 802.11g	
DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

**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.**

## Wi-Fi Protected Access

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

## 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.

## WEP Encryption

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

## IEEE 802.1x Network Security

The ZyAIR supports the IEEE 802.1x standard to enhance user authentication. Use the built-in user profile database to authenticate up to 32 users using MD5 encryption. Use an EAP-compatible RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate a limitless number of users using EAP (Extensible Authentication Protocol). EAP is an authentication protocol that supports multiple types of authentication.

## SNMP

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

## Full Network Management

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

## Logging and Tracing

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

## Embedded FTP and TFTP Servers

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

## Wireless Association List

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

## Wireless LAN Channel Usage

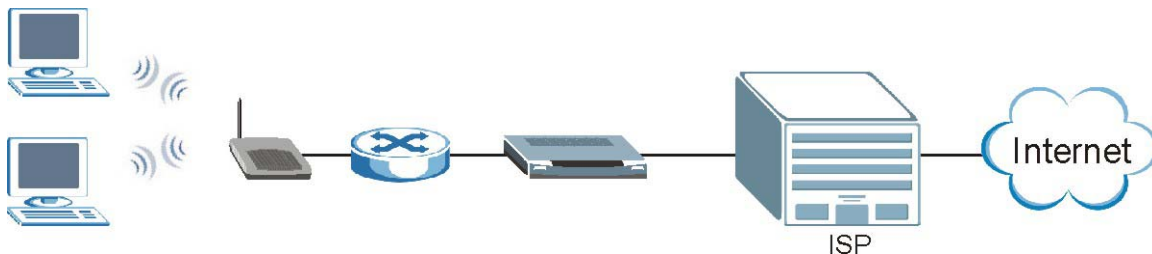
The **Wireless Channel Usage** screen displays whether the radio channels are used by other wireless devices within the transmission range of the ZyAIR. This allows you to select the channel with minimum interference for your ZyAIR.

## 1.3 Applications for the ZyAIR

Here are some 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.



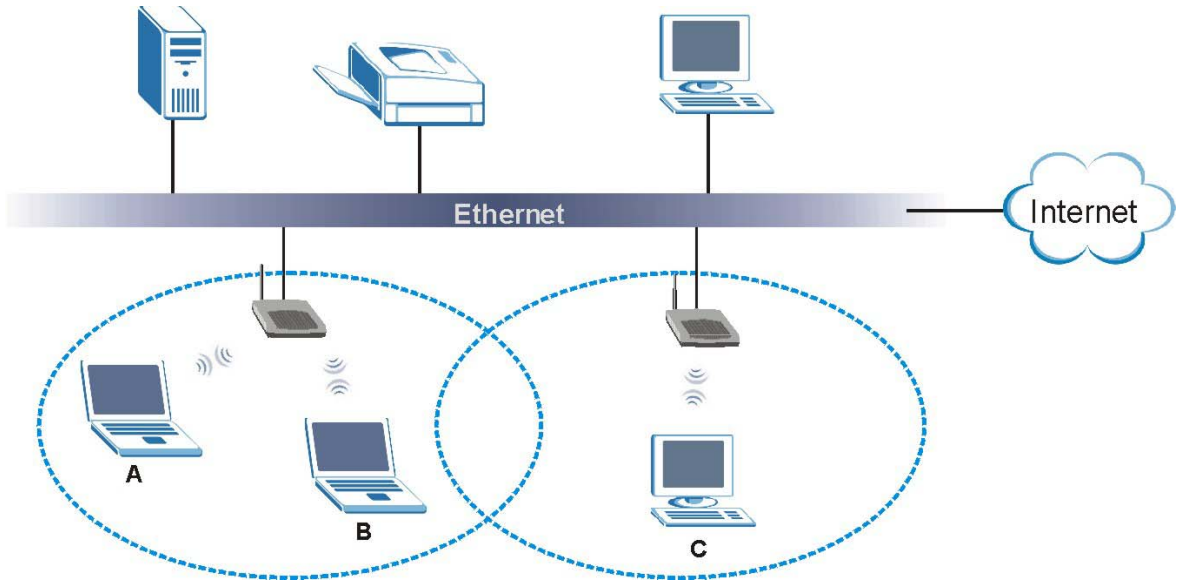
**Figure 1-1 Internet Access Application**

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





**Figure 1-2 Corporation Network Application**



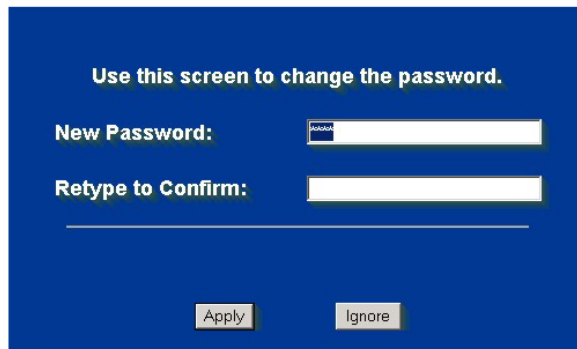
# Chapter 2

## 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.



Use this screen to change the password.

New Password:

Retype to Confirm:

**Figure 2-1 Change Password Screen**

- Step 7.** You should now see the **SYSTEM** screen.

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

## 2.2 Resetting the ZyAIR

If you forget your password or cannot access the 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:

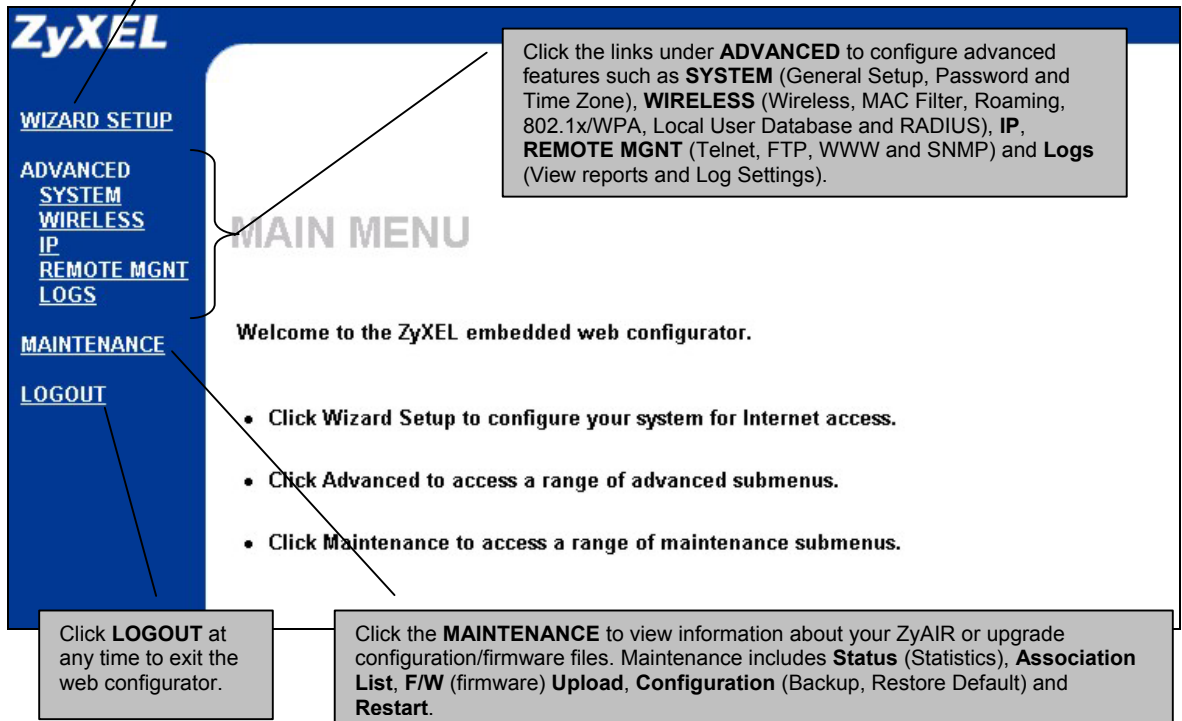
1. Use the **RESET** button on the top panel of the ZyAIR to upload the default configuration file (hold this button in for about 10 seconds or until the PWR/SYS LED turns red). Use this method for cases when the password or IP address of the ZyAIR is not known.
2. Use the web configurator to restore defaults (refer to the chapter on maintenance).
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

The following summarizes how to navigate the web configurator.

Follow the instructions below or click the  icon (located in the top right corner of most screens) to view online help.

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



**ZyXEL**

**WIZARD SETUP**

**ADVANCED**

**SYSTEM**

**WIRELESS**

**IP**

**REMOTE MGNT**

**LOGS**

**MAINTENANCE**

**LOGOUT**

**MAIN MENU**

Welcome to the ZyXEL embedded web configurator.

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

Click the links under **ADVANCED** to configure advanced features such as **SYSTEM** (General Setup, Password and Time Zone), **WIRELESS** (Wireless, MAC Filter, Roaming, 802.1x/WPA, Local User Database and RADIUS), **IP**, **REMOTE MGNT** (Telnet, FTP, WWW and SNMP) and **Logs** (View reports and Log Settings).

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

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

Figure 2-2 Navigating the ZyAIR Web Configurator



# Chapter 3

## Wizard Setup

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

### 3.1 Wizard Setup Overview

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

#### 3.1.1 Channel

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

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

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

#### 3.1.2 ESS ID

An Extended Service Set (ESS) is a group of access points connected to a wired LAN on the same subnet. An 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"> <li>➤ In Windows 95/98 click <b>Start, Settings, Control Panel, Network</b>. Click the Identification tab, note the entry for the <b>Computer Name</b> field and enter it as the <b>System Name</b>.</li> <li>➤ In Windows 2000, click <b>Start, Settings, Control Panel</b> and then double-click <b>System</b>. Click the <b>Network Identification</b> tab and then the <b>Properties</b> button. Note the entry for the <b>Computer name</b> field and enter it as the <b>System Name</b>.</li> <li>➤ In Windows XP, click <b>Start, My Computer, View system information</b> and then click the <b>Computer Name</b> tab. Note the entry in the <b>Full computer name</b> field and enter it as the ZyAIR <b>System Name</b>.</li> </ul> <p>This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.</p>

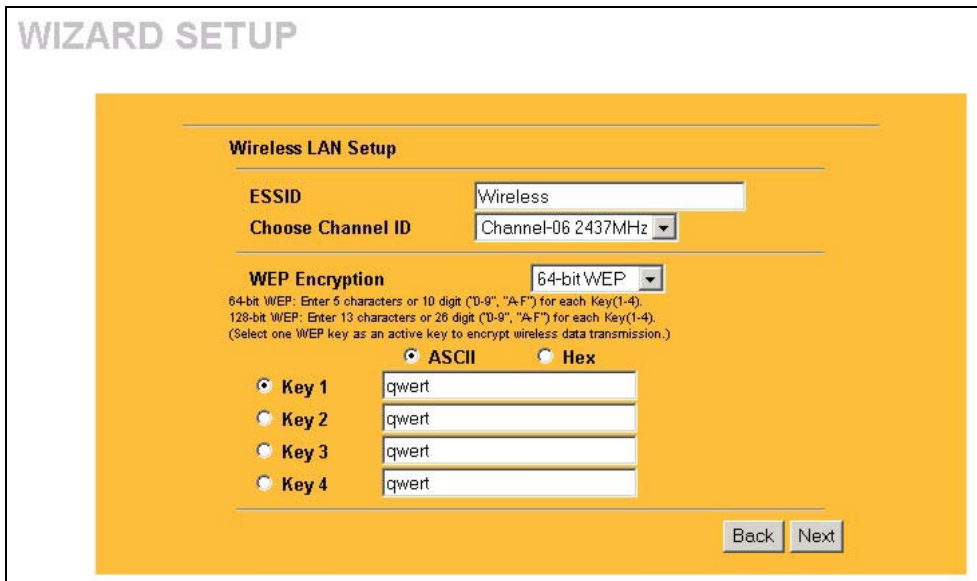


**Table 3-1 Wizard 1 : General Setup**

LABEL	DESCRIPTION
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Next	Click <b>Next</b> to proceed to the next screen.

### 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	

**Table 3-2 Wizard 2 : Wireless LAN Setup**

LABEL	DESCRIPTION
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	Select a channel from the drop-down list box.
WEP Encryption	Select <b>Disable</b> allows all wireless computers to communicate with the access points without any data encryption.  Select <b>64-bit WEP</b> or <b>128-bit WEP</b> 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 <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").  You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

## 3.4 Wizard Setup: IP Address

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

### 3.4.1 IP Address Assignment

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

**Table 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

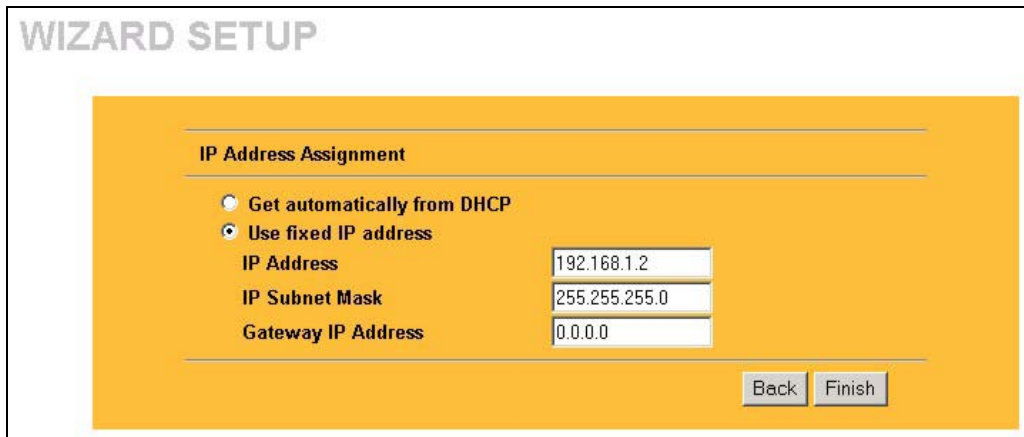
Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

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. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

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

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



**Figure 3-3 Wizard 3 : IP Address Assignment**

The following table describes the labels in this screen.

**Table 3-4 Wizard 3 : IP Address Assignment**

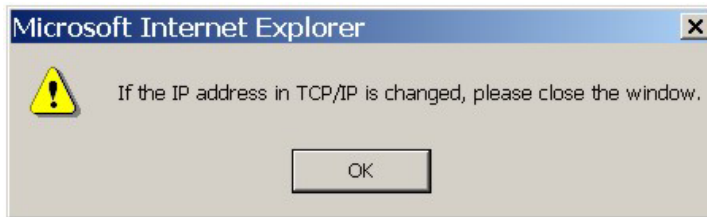
LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option if your ZyAIR is using a dynamically assigned IP address from a DHCP server each time.  <div style="border: 1px solid black; background-color: #cccccc; padding: 5px; text-align: center;"> <b>You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again.</b> </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 style="border: 1px solid black; background-color: #cccccc; padding: 5px; text-align: center;"> <b>If you change the ZyAIR's IP address, you must use the new IP address if you want to access the web configurator again.</b> </div>
IP Subnet Mask	Enter the subnet mask.

**Table 3-4 Wizard 3 : IP Address Assignment**

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of a 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 <b>Back</b> to return to the previous screen.
Finish	Click <b>Finish</b> 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.



## WIZARD SETUP

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

**Having Internet Access problems?**

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

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

---

# Part II:

---

## **SYSTEM, WIRELESS AND IP**

---

This part covers the information and web configurator screens of System, Wireless 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 **SYSTEM** to open the **General** screen.

**SYSTEM**

General Password Time Setting

System Name G-500

Domain Name

Administrator Inactivity Timer 60 (minutes, 0 means no timeout)

System DNS Servers

First DNS Server From DHCP 0.0.0.0

Second DNS Server None 0.0.0.0

Third DNS Server None 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 <b>From DHCP</b> 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 <b>User-Defined</b> 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 <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . Select <b>None</b> 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 <b>None</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

### 4.3 Configuring Password

To change your ZyAIR's password (recommended), click **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 section on resetting the ZyAIR for details.

The screenshot shows a web interface for password configuration. At the top, the word 'PASSWORD' is displayed in a large, light grey font. Below this, there are three tabs: 'General', 'Password', and 'Time Setting'. The 'Password' tab is currently selected and highlighted in yellow. The main content area is a solid yellow rectangle. It contains three text input fields stacked vertically, each preceded by a label: 'Old Password', 'New Password', and 'Retype to Confirm'. At the bottom of the yellow area, there are two buttons: 'Apply' and '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 <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 4.4 Configuring Time Setting

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

**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><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.</p> <p><b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>The default, <b>NTP (RFC 1305)</b>, is similar to Time (RFC 868).</p> <p>Select <b>None</b> 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 <b>None</b> in the <b>Time Protocol</b> field, enter the new time in this field and then click <b>Apply</b> .
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 <b>None</b> in the <b>Time Protocol</b> field, enter the new date in this field and then click <b>Apply</b> .
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 <b>Daylight Savings</b> .
End Date (mm-dd)	Enter the month and day that your daylight-savings time ends on if you selected <b>Daylight Savings</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.



# Chapter 5

## Wireless Configuration and Roaming

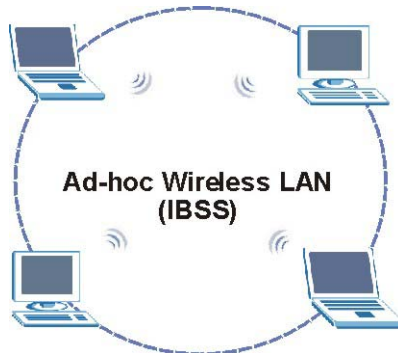
*This chapter discusses how to configure Wireless and Roaming screens on the ZyAIR.*

### 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).

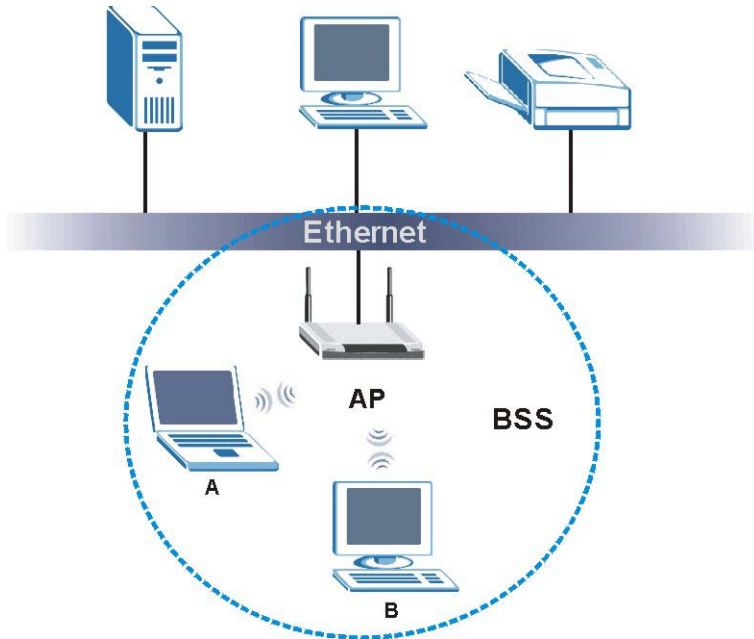


**Figure 5-1 IBSS (Ad-hoc) Wireless LAN**

#### 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.



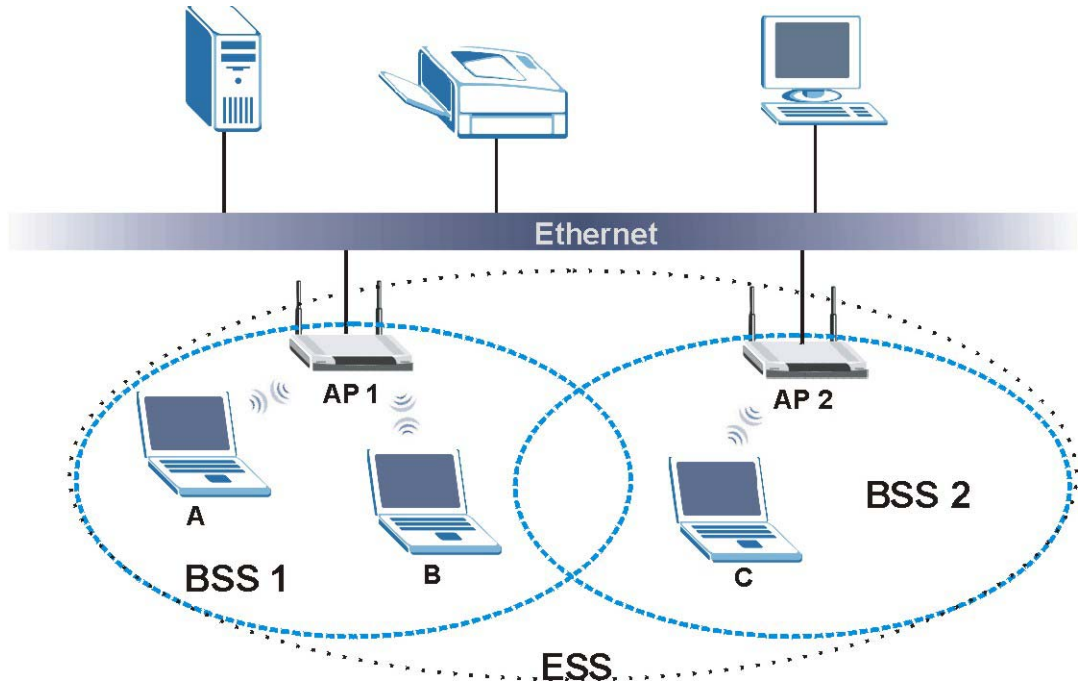


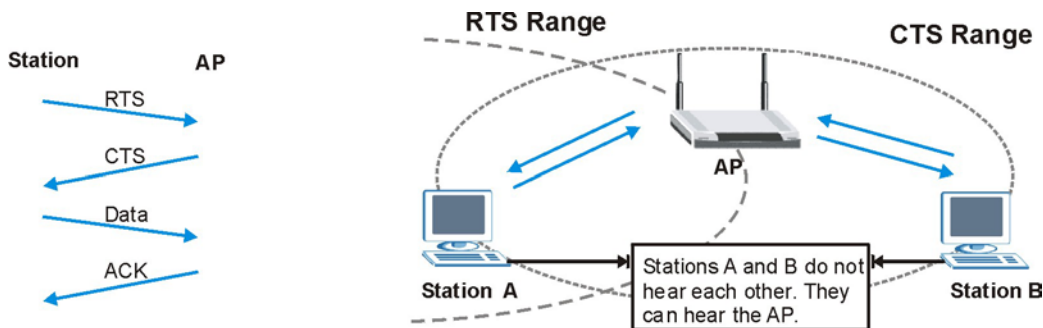
Figure 5-3 Extended Service Set

## 5.2 Wireless LAN Basics

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

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

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

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

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

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

**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 the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen.

### WIRELESS LAN

<b>Wireless</b>	<b>MAC Filter</b>	<b>Roaming</b>	<b>802.1x/WPA</b>	<b>Local User Database</b>	<b>RADIUS</b>
-----------------	-------------------	----------------	-------------------	----------------------------	---------------

---

**ESSID** Wireless

**Hide ESSID**

**Choose Channel ID** Channel-06 2437MHz

**RTS/CTS Threshold** 2432 (0 ~ 2432)

**Fragmentation Threshold** 2432 (256 ~ 2432)

---

**WEP Encryption** Disable

**Authentication Method** Auto

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

**ASCII**     **Hex**

**Key 1**

**Key 2**

**Key 3**

**Key 4**

---

**Preamble** Long

**802.11 Mode** Mixed

**Max. Frame Burst** 650 (0 ~1800)

---

Figure 5-5 Wireless

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

**Table 5-1 Wireless**

LABEL	DESCRIPTION
ESSID	<p>(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.</p> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <p><b>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.</b></p> </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. Select a channel from the drop-down list box. Refer to the chapter on wizard setup for more information about channels.
RTS/CTS Threshold	Enter a value between 0 and 2432. The default is <b>2432</b> .
Fragmentation Threshold	Enter a value between 256 and 2432. The default is <b>2432</b> . It is the maximum data fragment size that can be sent.
Apply	Click <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

See the chapter on wireless security for information on the other labels in this screen.

## 5.4 Configuring Roaming

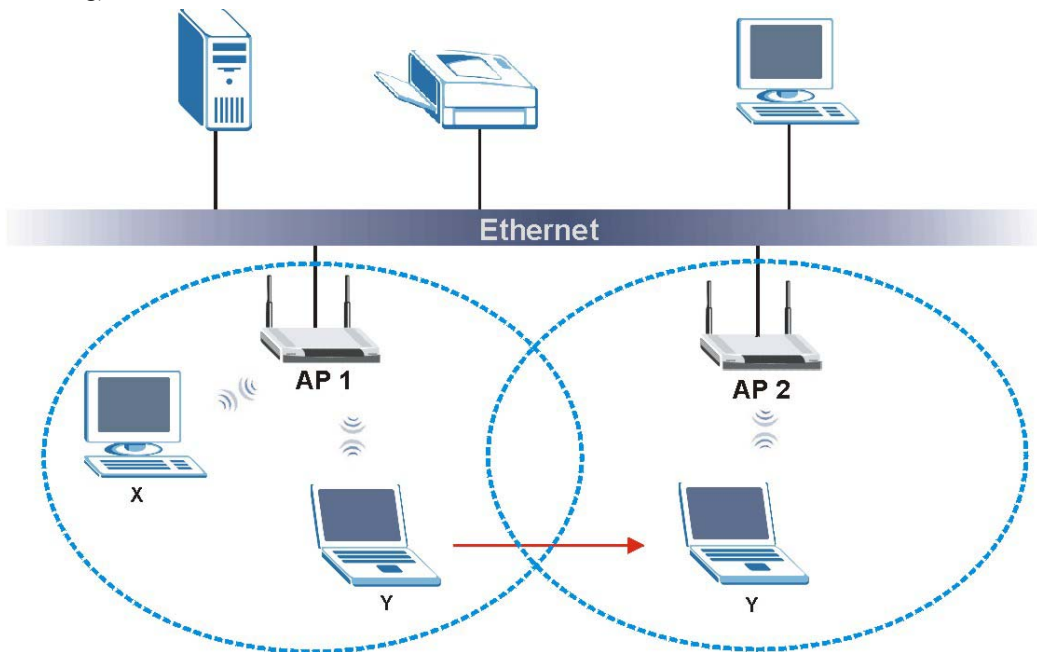
A wireless station is a device with an IEEE 802.11b compliant wireless adapters. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access 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 5-6*.

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

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



**Figure 5-6 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.

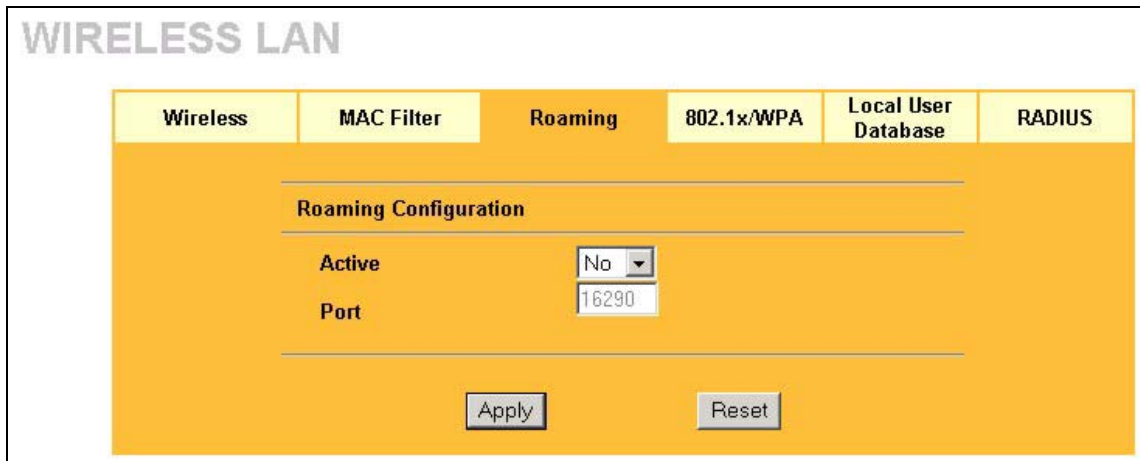
**Step 4.** Wireless station **Y** sends a request to access point **AP 2** for reauthentication.

### 5.4.1 Requirements for Roaming

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

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3. The adjacent access points should use different radio channels when their coverage areas overlap.
4. All access points must use the same port number to relay roaming information.
5. The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

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



**Figure 5-7 Roaming**

The following table describes the labels in this screen.

**Table 5-2 Roaming**

<b>LABEL</b>	<b>DESCRIPTION</b>
Active	Select <b>Yes</b> from the drop-down list box to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet. <div data-bbox="341 341 1220 411" style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; text-align: center;"><b>All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming.</b></div>
Port	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is <b>16290</b> . Make sure this port is not used by other services.
Apply	Click <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.





# Chapter 6

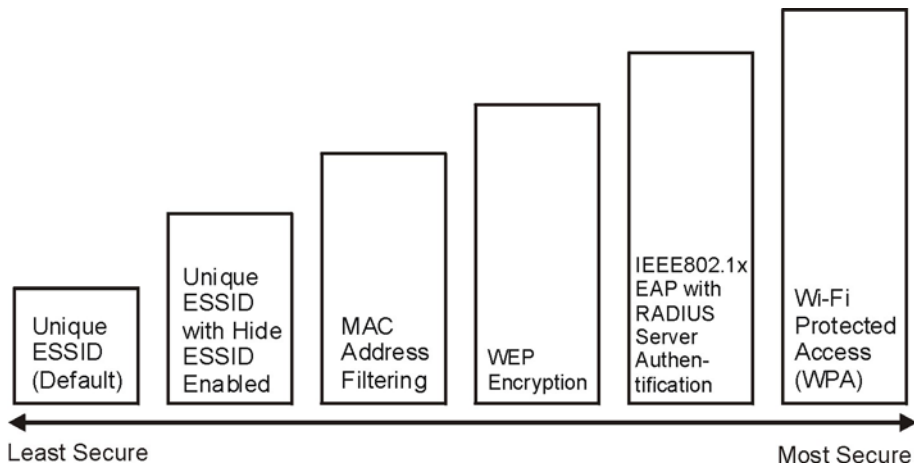
## Wireless Security

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



**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

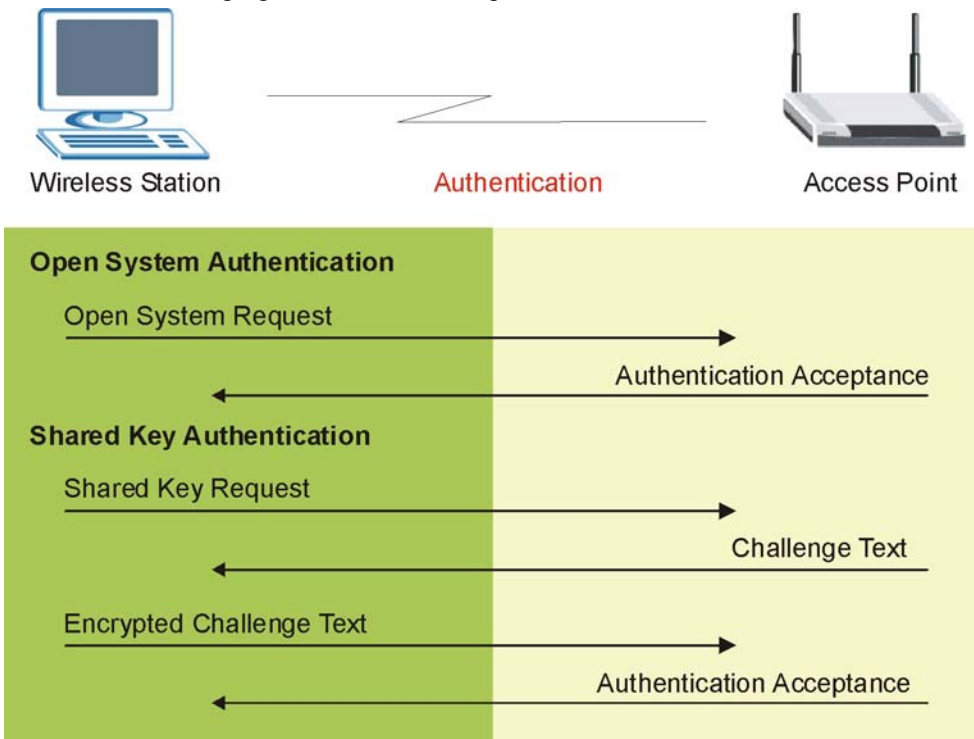
WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

## 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 Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless clients support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless clients support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the ZyAIR and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Auto** to have the ZyAIR automatically use short preamble when all wireless clients support it, otherwise the ZyAIR uses long preamble.

**The ZyAIR and the wireless stations MUST use the same preamble mode in order to communicate.**

## 6.4 Configuring WEP Encryption

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

**The WEP Encryption, Authentication Method and the WEP key fields are not visible when you enable Dynamic WEP Key, WPA or WPA-PSK in the 802.1x/WPA screen.**

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 <b>Disable</b> to allow wireless stations to communicate with the access points without any data encryption. Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.

**Table 6-1 Wireless**

LABEL	DESCRIPTION
Authentication Method	<p>Select <b>Auto</b>, <b>Open System</b> or <b>Shared Key</b> from the drop-down list box.</p> <p>This field is not available if WEP is not activated.</p> <p>If WEP encryption is activated, the default setting is <b>Auto</b>.</p>
ASCII	<p>Select this option to enter ASCII characters as the WEP keys.</p>
Hex	<p>Select this option to enter hexadecimal characters as the WEP keys.</p> <p>The preceding "0x" is entered automatically.</p>
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 <b>64-bit WEP</b>, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose <b>128-bit WEP</b>, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p>
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are <b>Long</b>, <b>Short</b> and <b>Auto</b>. The default setting is <b>Auto</b>.</p> <p>See the section on preamble for more information.</p>
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR.</p> <p>Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced.</p>
Max. Frame Burst	<p>Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in micro-seconds, that the ZyAIR transmits IEEE 802.11g wireless traffic only.</p> <p>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the ZyAIR.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 6.5 MAC Filter

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

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

**WIRELESS LAN**

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

---

**MAC Address Filter**

Active    No ▾

Filter Action    Allow Association ▾

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

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 <b>Yes</b> from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select <b>Deny Association</b> to block access to the ZyAIR, MAC addresses not listed will be allowed to access the ZyAIR. Select <b>Allow Association</b> to permit access to the ZyAIR, MAC addresses not listed will be denied access to the ZyAIR.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the ZyAIR in these address fields.
Apply	Click <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 6.6 802.1x Overview

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

## 6.7 Introduction to RADIUS

RADIUS is based on a client-sever 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.

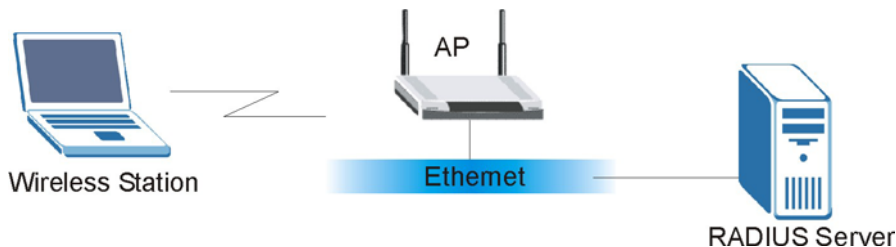
## 6.7.1 EAP Authentication Overview

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 PEAP 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.

## 6.8 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 6.17*) 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.**

## 6.9 Introduction to WPA

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

### 6.9.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can't use the ZyAIR's Local User Database for WPA authentication purposes since the Local User Database uses EAP-MD5 which cannot be used to generate keys. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS and EAP. Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

### 6.9.2 Encryption

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

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

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

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

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

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

## 6.10 WPA-PSK Application Example

A WPA-PSK application looks as follows.

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

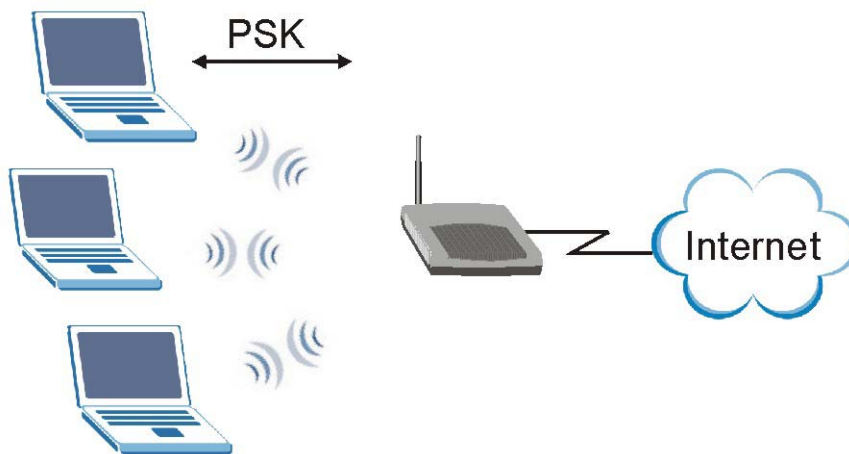


Figure 6-6 WPA - PSK Authentication

## 6.11 WPA with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. “A” is the RADIUS server. “DS” is the distribution system.

- Step 1.** The AP passes the wireless client's authentication request to the RADIUS server.
- Step 2.** The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- Step 3.** The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

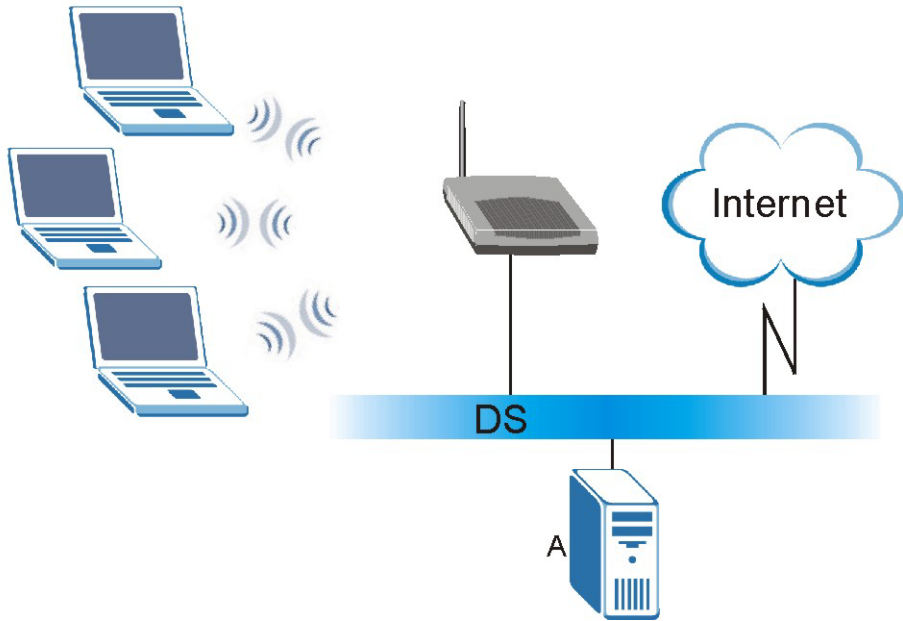


Figure 6-7 WPA with RADIUS Application Example

## 6.12 Security Parameters Summary

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

Table 6-3 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key

**Table 6-3 Wireless Security Relational Matrix**

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Enable
WPA	TKIP	No	Enable
WPA-PSK	WEP	Yes	Enable
WPA-PSK	TKIP	Yes	Enable

### 6.13 Wireless Client WPA Supplicants

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

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

### 6.14 Configuring 802.1x and WPA

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

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

**Figure 6-8 Wireless LAN: 802.1x/WPA**

The following table describes the labels in this screen.

**Table 6-4 Wireless LAN: 802.1x/WPA**

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 <b>No Access Allowed</b>, <b>No Authentication Required</b> and <b>Authentication Required</b>.</p> <p><b>No Access Allowed</b> blocks all wireless stations access to the wired network.</p> <p><b>No Authentication Required</b> allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting.</p> <p><b>Authentication Required</b> means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.</p> <p>Select <b>Authentication Required</b> to configure <b>Key Management Protocol</b> and other related fields.</p>

### 6.14.1 Authentication Required: 802.1x

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

**Figure 6-9 Wireless LAN: 802.1x/WPA for 802.1x Protocol**

The following table describes the labels in this screen.

**Table 6-5 Wireless LAN: 802.1x/WPA for 802.1x Protocol**

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 <b>No Authentication Required</b>, <b>Authentication Required</b> and <b>No Access Allowed</b>.</p> <p><b>No Authentication Required</b> allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting.</p> <p><b>Authentication Required</b> means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.</p> <p><b>No Access Allowed</b> blocks all wireless stations access to the wired network.</p> <p>The following fields are only available when you select <b>Authentication Required</b>.</p>



**Table 6-5 Wireless LAN: 802.1x/WPA for 802.1x Protocol**

LABEL	DESCRIPTION
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 <b>Authentication Required</b> in the <b>Wireless Port Control</b> field.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes).</p> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <p><b>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</b></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 <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. The default time interval is <b>3600</b> seconds (or 1 hour).</p>
Key Management Protocol	<p>Choose <b>802.1x</b> from the drop-down list.</p>
Dynamic WEP Key Exchange	<p>This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Also set the <b>Authentication Databases</b> field to <b>RADIUS Only</b>. Local user database may not be used.</p> <p>Select <b>Disable</b> to allow wireless stations to communicate with the access points without using dynamic WEP key exchange.</p> <p>Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.</p> <p>Up to 32 stations can access the ZyAIR when you configure dynamic WEP key exchange.</p> <p>This field is not available when you set <b>Key Management Protocol</b> to <b>WPA</b> or <b>WPA-PSK</b>.</p>

**Table 6-5 Wireless LAN: 802.1x/WPA for 802.1x Protocol**

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

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

### 6.14.2 Authentication Required: WPA

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

**WIRELESS LAN**

Wireless	MAC Filter	Roaming	802.1x/WPA	Local User Database	RADIUS
<b>802.1X Authentication</b>					
<b>Wireless Port Control</b>				Authentication Required ▾	
<b>ReAuthentication Timer</b>				1800 (In Seconds)	
<b>Idle Timeout</b>				3600 (In Seconds)	
<b>Key Management Protocol</b>				WPA ▾	
<b>WPA Mixed Mode</b>				Disable ▾	
<b>WPA Group Key Update Timer</b>				1800 (seconds)	
<b>Authentication Databases</b>				RADIUS Only ▾	
			Apply		
			Reset		

**Figure 6-10 Wireless LAN: 802.1x/WPA for WPA Protocol**

The following table describes the labels not previously discussed

**Table 6-6 Wireless LAN: 802.1x/WPA for WPA Protocol**

LABEL	DESCRIPTION
Key Management Protocol	Choose <b>WPA</b> in this field.
WPA Mixed Mode	The ZyAIR can operate in <b>WPA Mixed Mode</b> , which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select <b>Enable</b> to activate WPA mixed mode. Otherwise, select <b>Disable</b> .
WPA Group Key Update Timer	The <b>WPA Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or RADIUS server (if using <b>WPA</b> key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Group Key Update Timer</b> is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).

**Table 6-6 Wireless LAN: 802.1x/WPA for WPA Protocol**

LABEL	DESCRIPTION
Authentication Databases	When you configure <b>Key Management Protocol</b> to <b>WPA</b> , the <b>Authentication Databases</b> must be <b>RADIUS Only</b> . You can only use the <b>Local User Database Only</b> with <b>802.1x Key Management Protocol</b> .

### 6.14.3 Authentication Required: WPA-PSK

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

**WIRELESS LAN**

Wireless | MAC Filter | Roaming | **802.1x/WPA** | Local User Database | RADIUS

**802.1X Authentication**

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA-PSK

Pre-Shared Key: [Empty]

WPA Mixed Mode: Enable

WPA Group Key Update Timer: 1800 (seconds)

Authentication Databases: RADIUS Only

Apply | Reset

**Figure 6-11 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol**

The following table describes the labels not previously discussed

**Table 6-7 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol**

LABEL	DESCRIPTION
Key Management Protocol	Choose <b>WPA-PSK</b> in this field.
Pre-Shared Key	The encryption mechanisms used for <b>WPA</b> and <b>WPA-PSK</b> are the same. The only difference between the two is that <b>WPA-PSK</b> uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
WPA Mixed Mode	The ZyAIR can operate in <b>WPA Mixed Mode</b> , which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select <b>Enable</b> to activate WPA mixed mode. Otherwise, select <b>Disable</b> .
WPA Group Key Update Timer	The <b>WPA Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or RADIUS server (if using <b>WPA</b> key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Group Key Update Timer</b> is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).
Authentication Databases	This field is only visible when <b>WPA Mixed Mode</b> is enabled. When you configure <b>Key Management Protocol</b> to <b>WPA</b> , the <b>Authentication Databases</b> must be <b>RADIUS Only</b> . You can only use the <b>Local User Database Only</b> with <b>802.1x Key Management Protocol</b> .

## 6.15 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.

## 6.16 Configuring Local User Database

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

WIRELESS LAN

Wireless    MAC Filter    Roaming    802.1x/WPA    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 6-12 Local User Database**

The following table describes the labels in this screen.

**Table 6-8 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 <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 6.17 Configuring RADIUS

Configure the **RADIUS** screen if you want to authenticate wireless users using an external server.

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

**WIRELESS LAN**

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

---

**Authentication Server**

Active: No

Server IP Address: 0.0.0.0

Port Number: 1812

Shared Secret: \_\_\_\_\_

---

**Accounting Server**

Active: No

Server IP Address: 0.0.0.0

Port Number: 1813

Shared Secret: \_\_\_\_\_

Apply    Reset

**Figure 6-13 RADIUS**

The following table describes the labels in this screen.

**Table 6-9 RADIUS**

LABEL	DESCRIPTION
Authentication Server	
Active	Select <b>Yes</b> from the drop-down list box to enable user authentication through an external authentication server. Select <b>No</b> 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 <b>1812</b> . 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 <b>Yes</b> 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 <b>1813</b> . 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 <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# Chapter 7

## IP Screen

*This chapter discusses how to configure IP on the ZyAIR*

### 7.1 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.

### 7.2 TCP/IP Parameters

#### 7.2.1 IP Address and Subnet Mask

Refer to the section on IP address and subnet mask in the *Wizard Setup* chapter for this information.

### 7.3 Configuring IP

Click **IP** to display the screen shown next.

The screenshot shows a configuration window with a yellow background. At the top left, the word "IP" is displayed in a large, light grey font. Below it, the word "IP" appears again in a smaller, bold black font. The main content area is titled "IP Address Assignment" and contains two radio button options. The first option, "Get automatically from DHCP", is unselected. The second option, "Use fixed IP address", is selected. Below these options are three input fields: "IP Address" containing "192.168.1.2", "IP Subnet Mask" containing "255.255.255.0", and "Gateway IP Address" containing "0.0.0.0". At the bottom of the form are two buttons: "Apply" and "Reset".

**Figure 7-1 IP Setup**

The following table describes the labels in this screen.

**Table 7-1 IP Setup**

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	<p>Select this option if your ZyAIR is using a dynamically assigned IP address from a DHCP server each time.</p> <p style="text-align: center;"><b>You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again.</b></p>
Use fixed IP address	<p>Select this option if your ZyAIR is using a static IP address. When you select this option, fill in the fields below.</p>
IP Address	<p>Enter the IP address of your ZyAIR in dotted decimal notation.</p> <p style="text-align: center;"><b>If you change the ZyAIR's IP address, you must use the new IP address if you want to access the web configurator again.</b></p>
IP Subnet Mask	<p>Enter the subnet mask.</p>
Gateway IP Address	<p>Enter the IP address of a 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.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the ZyAIR.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

---

# Part III:

---

## **REMOTE MANAGEMENT AND LOGS**

---

This part provides information and configuration instructions for Remote Management and the logs.



# Chapter 8

## Remote Management

*This chapter provides information on the Remote Management screens.*

### 8.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyAIR interface (if any) from which computers. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your ZyAIR from a remote location via:

- WLAN only,
- ALL (LAN and WLAN),
- LAN only,
- Neither (Disable).

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

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

1. Console port
2. Telnet
3. HTTP

#### 8.1.1 Remote Management Limitations

Remote management over LAN or WLAN will not work when:

1. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

#### 8.1.2 System Timeout

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

## 8.2 Telnet

You can telnet into the ZyAIR to perform remote management.

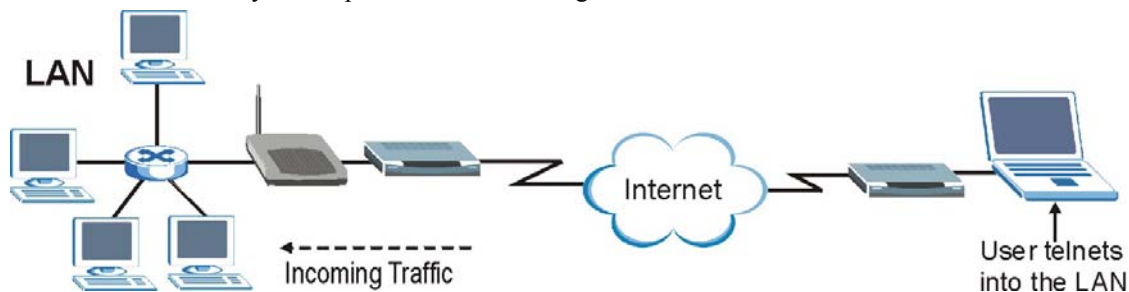


Figure 8-1 Telnet Configuration on a TCP/IP Network

## 8.3 Configuring TELNET

Click **REMOTE MGNT** to open the **TELNET** screen.

Figure 8-2 Telnet

The following table describes the labels in this screen.

Table 8-1 Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

**Table 8-1 Telnet**

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

## 8.4 Configuring FTP

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

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

The screenshot shows the 'REMOTE MANAGEMENT' interface with the 'FTP' tab selected. The configuration fields are as follows:

- Server Port:** 21
- Server Access:** WLAN & LAN
- Secured Client IP Address:** All (selected), Selected, 0.0.0.0

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

**Figure 8-3 FTP**

The following table describes the labels in this screen.

**Table 8-2 FTP**

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

## 8.5 Configuring WWW

To change your ZyAIR's World Wide Web settings, click **REMOTE MGNT** and then the **WWW** tab. The screen appears as shown.

The screenshot shows the 'REMOTE MANAGEMENT' interface with the 'WWW' tab selected. The configuration options are as follows:

- Server Port:** 80
- Server Access:** WLAN & LAN
- Secured Client IP Address:** All (selected), Selected, 0.0.0.0

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

**Figure 8-4 WWW**

The following table describes the labels in this screen.

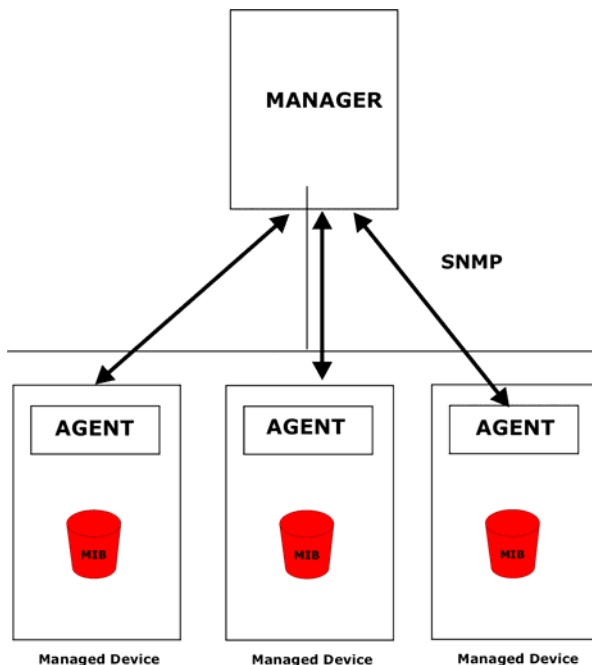


**Table 8-3 WWW**

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

## 8.6 Configuring 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 8-5 SNMP Management Model**

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

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

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include 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.

### 8.6.1 Supported MIBs

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

### 8.6.2 SNMP Traps

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

**Table 8-4 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 8-5 Ports and Interface Types**

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

### 8.6.3 REMOTE MANAGEMENT: SNMP

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

## REMOTE MANAGEMENT

TELNET
FTP
WWW
SNMP

### SNMP Configuration

---

Get Community

Set Community

Trap

Community

Destination

---

### SNMP

---

Service Port

Service Access

Secured Client IP Address  All  Selected

---

**Figure 8-6 SNMP**

The following table describes the labels in this screen.

**Table 8-6 SNMP**

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station.

**Table 8-6 SNMP**

LABEL	DESCRIPTION
Trusted Host	If you enter a trusted host, your ZyAIR will only respond to SNMP messages from this address. A blank (default) field means your ZyAIR will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	<p>A secured client is a “trusted” computer that is allowed to communicate with the ZyAIR using this service.</p> <p>Select <b>All</b> to allow any computer to access the ZyAIR using this service.</p> <p>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyAIR using this service.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyAIR.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# 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 **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.

The screenshot shows the 'View Log' interface. At the top, there are two tabs: 'View Log' and 'Log Settings'. Below the tabs, there is a 'Display' dropdown menu currently set to 'All Logs'. To the right of the dropdown are three buttons: 'Email Log Now', 'Refresh', and 'Clear Log'. Below these controls is a table with the following data:

#	Time ▲	Message	Source	Destination	Note
1	01/01/2000 01:13:58	User login from WEB successfully	192.168.1.10		User:admin
2	01/01/2000 01:09:40	User login from TELNET successfully	192.168.1.10		User:admin
3	01/01/2000 01:09:05	User login from WEB successfully	192.168.1.10		User:admin

Figure 9-1 View Log

The following table describes the labels in this screen.

**Table 9-1 View Log**

<b>LABEL</b>	<b>DESCRIPTION</b>
Display	Select a log category from the drop down list box to display logs within the selected category. To view all logs, select <b>All Logs</b> . The number of categories shown in the drop down list box depends on the selection in the <b>Log Settings</b> 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.
Note	This field displays additional information about the log entry.
Email Log Now	Click <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page.
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to clear all the logs.

## 9.2 Configuring Log Settings

To change your ZyAIR's log settings, click **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.



## Log Settings

**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)

---

**Syslog Logging:**

Active

Syslog IP Address:  (Server NAME or IP Address)

Log Facility:

---

**Send Log:**

Log Schedule:

Day for Sending Log:

Time for Sending Log:  (hour)  (minute)

Clear log after sending mail

---

<b>Log</b>	<b>Send immediate alert</b>
<input checked="" type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors
<input checked="" type="checkbox"/> System Errors	
<input checked="" type="checkbox"/> 802.1x	
<input checked="" type="checkbox"/> Wireless	

---

**Figure 9-2 Log Settings**

The following table describes the labels in this screen.

Table 9-2 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyAIR sends.
Send log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send alerts to	Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click <b>Active</b> to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
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"> <li>• <b>Daily</b></li> <li>• <b>Weekly</b></li> <li>• <b>Hourly</b></li> <li>• <b>When Log is Full</b></li> <li>• <b>None.</b></li> </ul> <p>If the <b>Weekly</b> or the <b>Daily</b> option is selected, specify a time of day when the E-mail should be sent. If the <b>Weekly</b> option is selected, then also specify which day of the week the E-mail should be sent. If the <b>When Log is Full</b> option is selected, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are sent.</p>
Day for Sending Log	This field is only available when you select <b>Weekly</b> in the <b>Log Schedule</b> 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.

**Table 9-2 Log Settings**

LABEL	DESCRIPTION
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select the categories of alerts for which you want the ZyAIR to immediately send e-mail alerts.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to reconfigure all the fields in this screen.



---

# Part IV:

---

## **MAINTENANCE**

---

This part describes the Maintenance web configurator screens.



# Chapter 10

## Maintenance

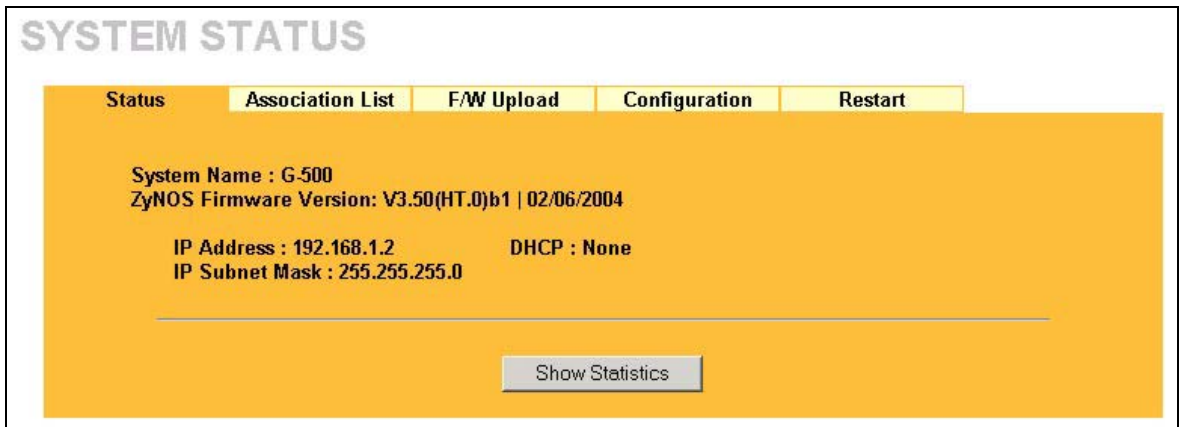
*This chapter describes the Maintenance screens that display system information such as ZyNOS firmware, port IP addresses and port traffic statistics.*

### 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 display the 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 <b>System Name</b> 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.
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 - <b>Client</b> or <b>None</b> .
Show Statistics	Click <b>Show Statistics</b> to see 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
LAN	100M/Full	1266	3861	0	0	0	1:35:47
WLAN	54M	2945	0	0	0	0	1:37:11

System Up Time : 1:37:17

Poll Interval(s) :  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.
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.



**Table 10-2 System Status: Show Statistics**

LABEL	DESCRIPTION
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 Association List

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

WIRELESS				
Status	Association List	F/W Upload	Configuration	Restart
#	MAC Address	Association Time		
001	00:02:d1:28:00:bc	00:36:17 2000/01/01		
002	00:a0:c5:46:cd:4a	01:06:27 2000/01/01		

Refresh

**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.
Refresh	Click <b>Refresh</b> to reload the screen.

## 10.4 F/W Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a ".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 the **F/W Upload** tab to display the screen as shown. Follow the instructions in this screen to upload firmware to your ZyAIR.



**Figure 10-4 Firmware Upload**

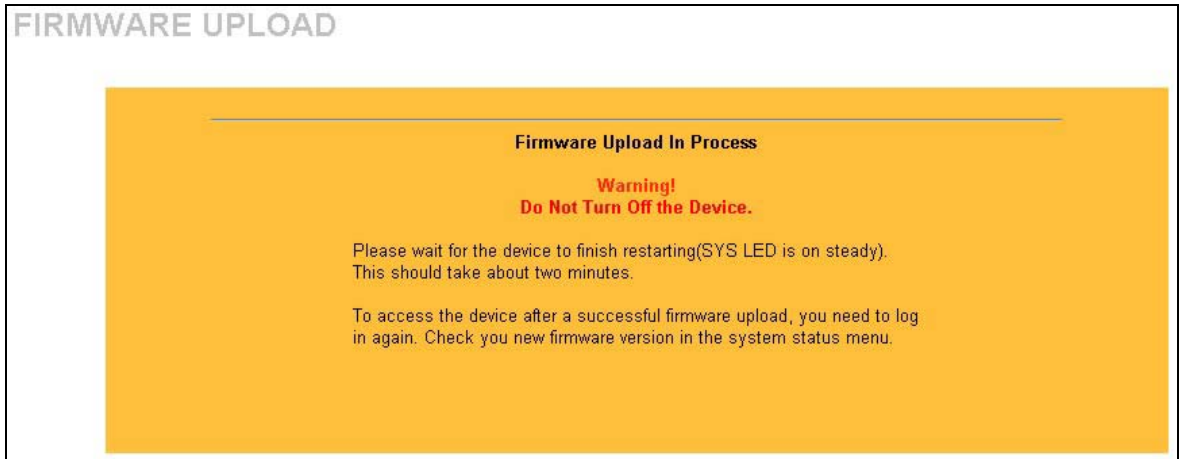
The following table describes the labels in this screen.

**Table 10-4 Firmware Upload**

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

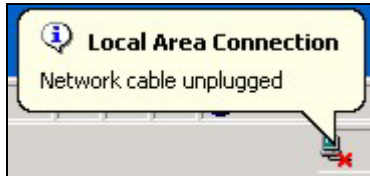
**Do not turn off the ZyAIR while firmware upload is in progress!**

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



**Figure 10-5 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 10-6 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.

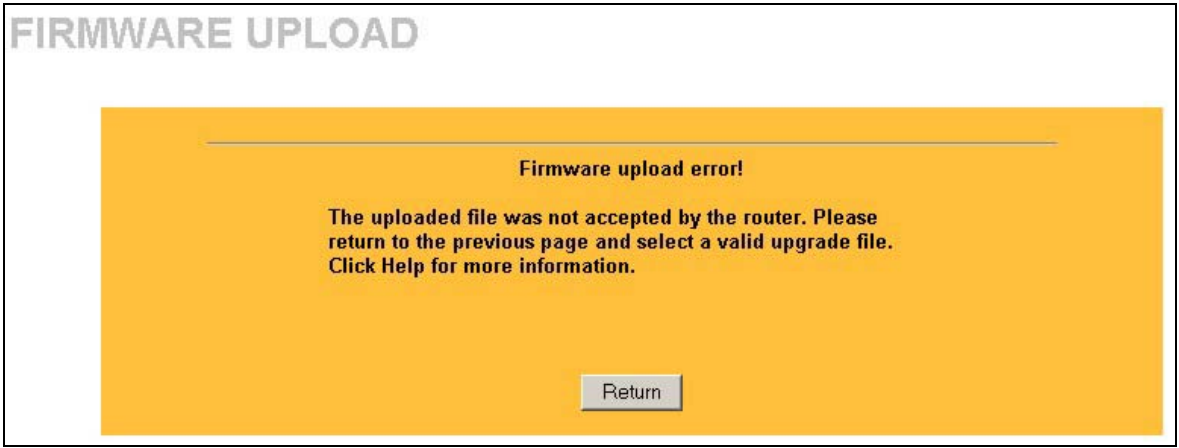


Figure 10-7 Firmware Upload Error

## 10.5 Configuration Screen

See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

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

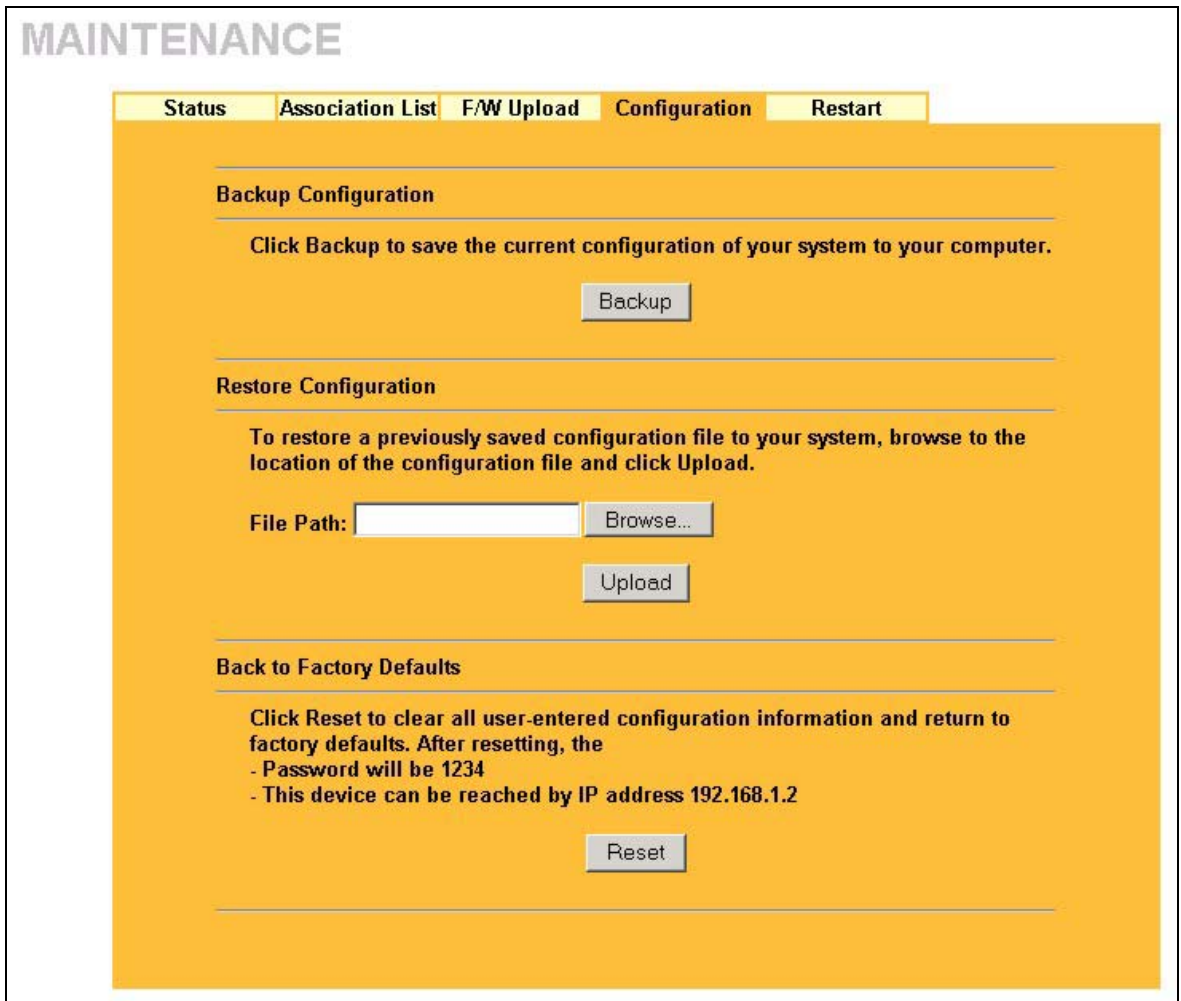


Figure 10-8 Configuration

### 10.5.1 Backup Configuration

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

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

## 10.5.2 Restore Configuration

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

**Table 10-5 Restore Configuration**

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

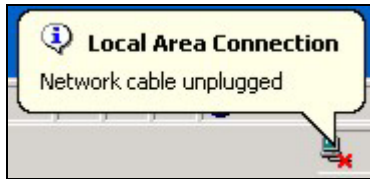
**Do not turn off the ZyAIR while configuration file upload is in progress.**

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



**Figure 10-9 Configuration Upload Successful**

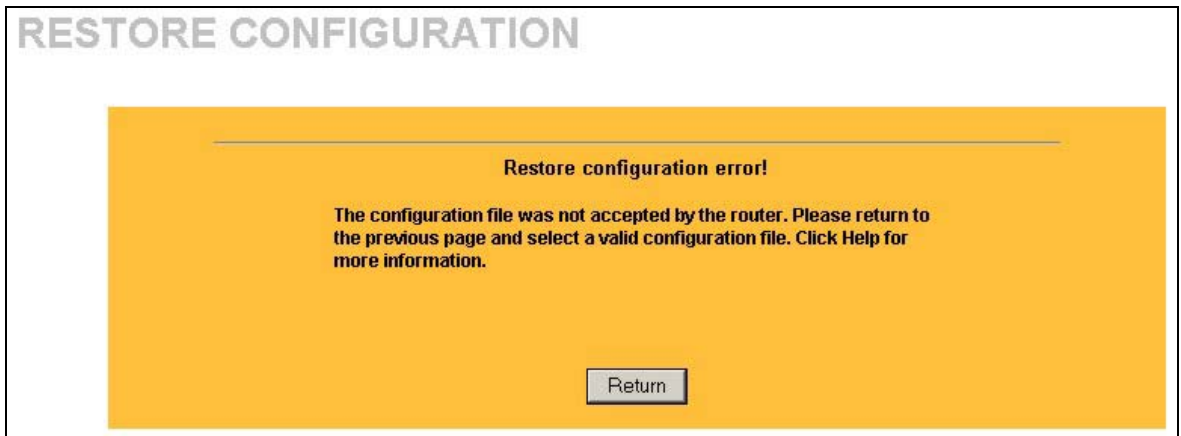
The ZyAIR automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.



**Figure 10-10 Network Temporarily Disconnected**

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

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

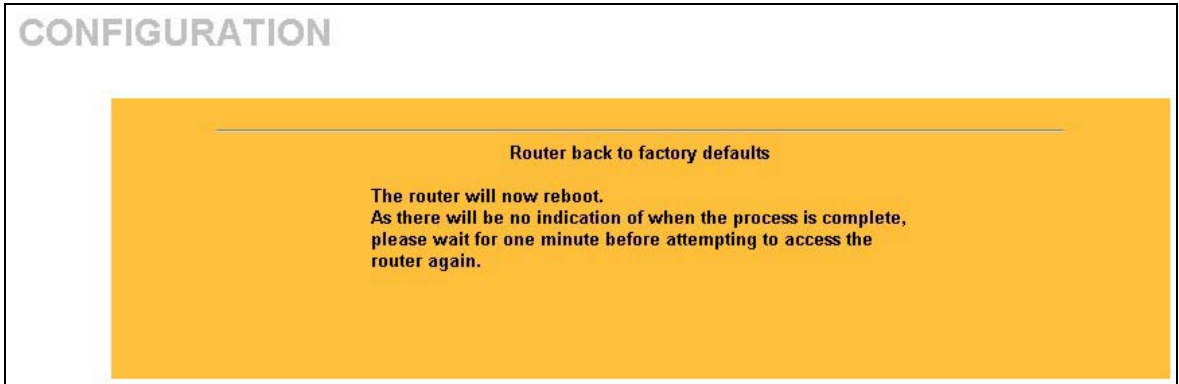


**Figure 10-11 Configuration Upload Error**

### 10.5.3 Back to Factory Defaults

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





**Figure 10-12 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 section on resetting the ZyAIR for more information on the **RESET** button.

## 10.6 Restart Screen

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

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



**Figure 10-13 Restart Screen**



---

---

# 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

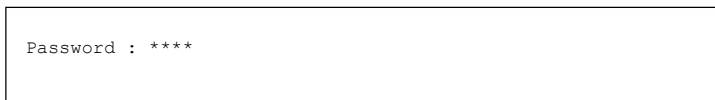
## Introducing the SMT

*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

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

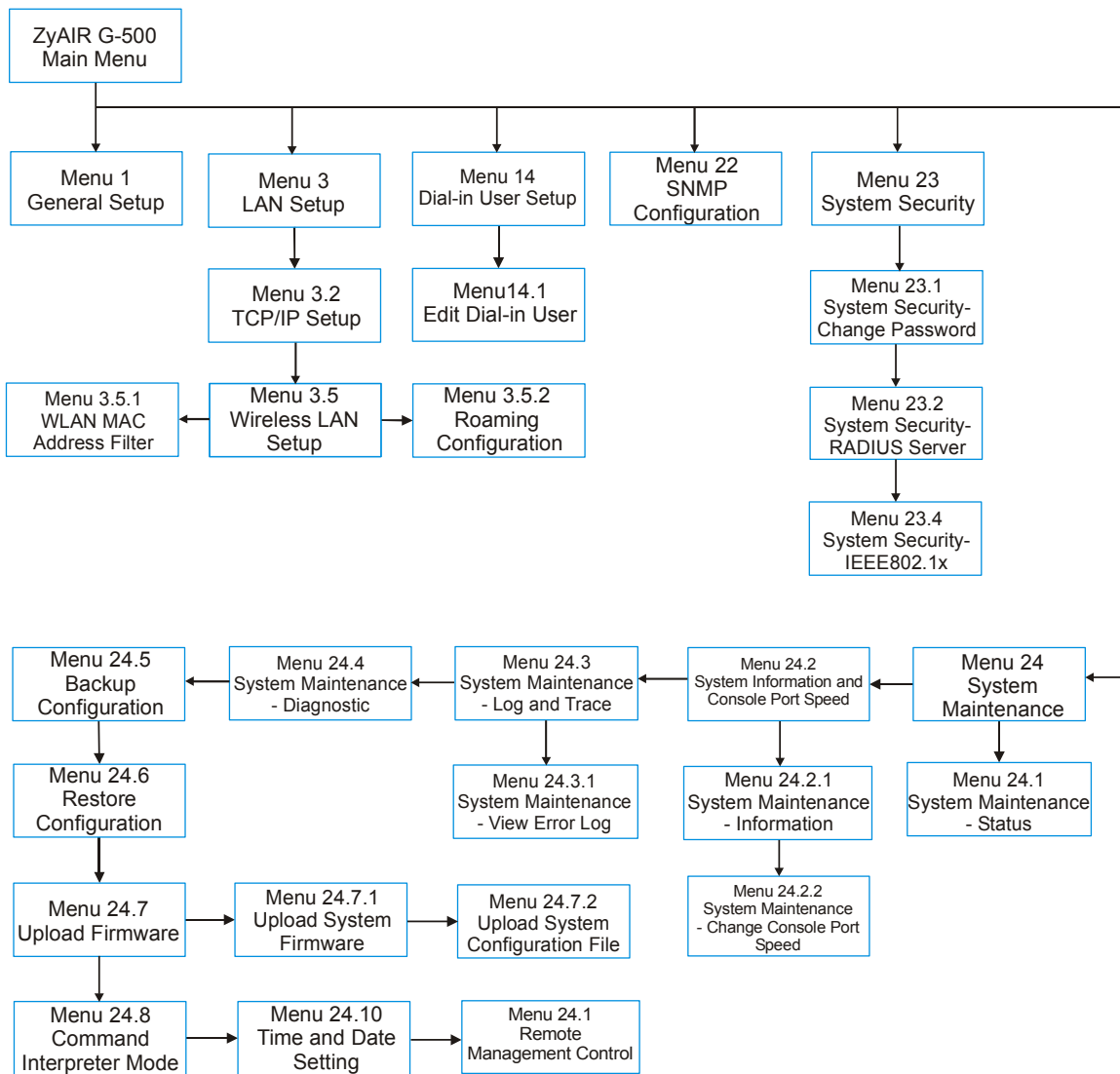


Figure 11-3 ZyAIR G-500 SMT Menu Overview Example

## 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 <b>No</b> to <b>Yes</b> then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of <b>No</b> . Press [SPACE BAR] once to change <b>No</b> to <b>Yes</b> , 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 <b>ChangeMe</b>	All fields with the symbol <?> must be filled in order to be able to save the new configuration.  All fields with <b>ChangeMe</b> 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.



```

Copyright (c) 1994 - 2003 ZyXEL Communications Corp.

                                ZyAIR G-500 Main Menu

Getting Started                                Advanced Management
  1. General Setup                            22. SNMP Configuration
  3. LAN Setup                                23. System Security
                                              24. System Maintenance

Advanced Applications
  14. Dial-in User Setup

                                              99. Exit

                                Enter Menu Selection Number:
    
```

**Figure 11-4 ZyAIR G-500 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.
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. This is not a required field. Leave this field blank or enter the domain name here if you know it.

#### 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=
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**

<b>FIELD</b>	<b>DESCRIPTION</b>	<b>EXAMPLE</b>
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.	G-500
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 <b>From DHCP</b> , <b>User Defined</b> or <b>None</b> and press [ENTER]. These fields are not available on all models.	<b>From DHCP</b>
IP Address	Enter the IP addresses of the DNS servers. This field is available when you select <b>User-Defined</b> in the field above.	<b>N/A</b>
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**

### 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 <b>Dynamic</b> 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 <b>Static</b> 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.

```

Menu 3.5 - Wireless LAN Setup

ESSID= Wireless
Hide ESSID= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP Encryption= 64-bit WEP
    Default Key= 1
    Key1= *****
    Key2= *****
    Key3= *****
    Key4= *****
    Authen. Method= Auto
Edit MAC Address Filter= No
Edit Roaming Configuration=
Preamble= Long
802.11 Mode= Mixed
Max. Frame Burst= 650

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

**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
ESSID	The ESSID (Extended Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the AP must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters.	Wireless
Hide ESSID	Press [SPACE BAR] and select <b>Yes</b> to hide the ESSID in the outgoing data frame so an intruder cannot obtain the ESSID through passive scanning.	<b>No</b>
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.	<b>CH01 2412MHz</b>
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.	<b>2432</b>
Frag. Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.	<b>2432</b>
WEP Encryption	Select <b>Disable</b> to allow wireless stations to communicate with the access points without any data encryption. Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.	<b>Disable</b>

**Table 13-2 Menu 3.5 Wireless LAN Setup**

FIELD	DESCRIPTION	EXMAPLE
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	<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 <b>64-bit WEP</b> in the <b>WEP Encryption</b> field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose <b>128-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p style="text-align: center;"><b>Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key.</b></p>	0x12345abcde
Authen. Method	<p>Press [SPACE BAR] to select <b>Auto</b>, <b>Open System Only</b> or <b>Shared Key Only</b> and press [ENTER].</p> <p>This field is <b>N/A</b> if WEP is not activated.</p> <p>If WEP encryption is activated, the default setting is <b>Auto</b>.</p>	<b>Auto</b>
Edit MAC Address Filter	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to display menu 3.5.1. See the section on MAC address filter for more information.	<b>No</b>
Edit Roaming Configuration	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to display menu 3.5.2. See the section on roaming configuration for more information.	<b>No</b>
Preamble	<p>Press [SPACE BAR] to select a preamble type. Choices are <b>Long</b>, <b>Short</b> and <b>Auto</b>. The default setting is <b>Auto</b>.</p> <p>See the section on preamble for more information.</p>	<b>Auto</b>
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR.</p> <p>Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced. This is the default setting.</p>	<b>Mixed</b>



**Table 13-2 Menu 3.5 Wireless LAN Setup**

FIELD	DESCRIPTION	EXMAPLE
Max. Frame Burst	<p>Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in micro-seconds, that the ZyAIR transmits IEEE 802.11g wireless traffic only.</p> <p>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.</p>	<b>650</b>
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.</p>		

### 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

ESSID= Wireless
Hide ESSID= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP Encryption= 64-bit WEP
  Default Key= 1
  Key1= *****
  Key2= *****
  Key3= *****
  Key4= *****
  Authen. Method= Auto
Edit MAC Address Filter= Yes
Edit Roaming Configuration=
Preamble= Long
802.11 Mode= Mixed
Max. Frame Burst= 650

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 13-4 Menu 3.5 Wireless LAN Setup**

**Step 3.** In the **Edit MAC Address Filter** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.1 – WLAN MAC Address Filter** displays as shown next.

```

Menu 3.5.1 - WLAN MAC Address Filter

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

Enter here to CONFIRM or ESC to CANCEL:

```

**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 <b>Yes</b> and press [ENTER].
Filter Action	<p>Define the filter action for the list of MAC addresses in the MAC address filter table.</p> <p>To deny access to the ZyAIR, press [SPACE BAR] to select <b>Deny Association</b> and press [ENTER]. MAC addresses not listed will be allowed to access the ZyAIR.</p> <p>The default action, <b>Allowed Association</b>, permits association with the ZyAIR. MAC addresses not listed will be denied access to the ZyAIR.</p>
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

ESSID= Wireless
Hide ESSID= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP Encryption= 64-bit WEP
  Default Key= 1
  Key1= *****
  Key2= *****
  Key3= *****
  Key4= *****
  Authen. Method= Auto

Edit MAC Address Filter= No
Edit Roaming Configuration= Yes
Preamble= Long
802.11 Mode= Mixed
Max. Frame Burst= 650

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 <b>Yes</b> 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 <b>16290</b> . Make sure this port is not used by other services.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

# Chapter 14

## Dial-in User Setup

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

### 14.1 Dial-in User Setup

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

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

**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 <b>Yes</b> and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

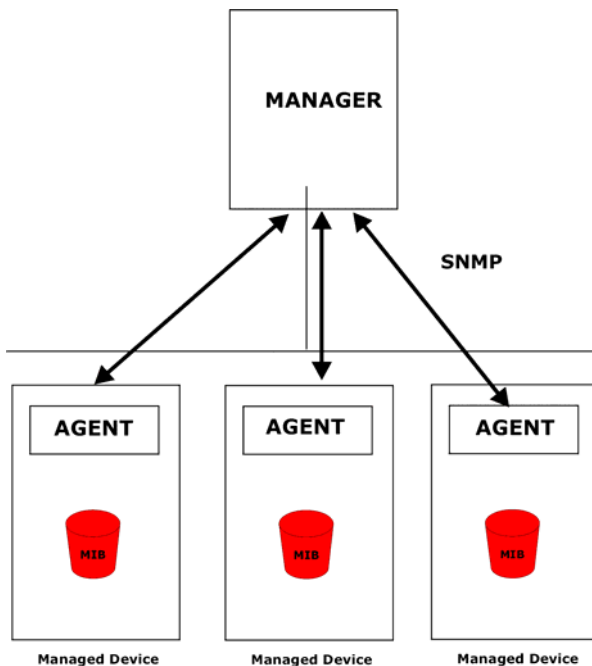
# Chapter 15

## SNMP Configuration

*This chapter explains SNMP Configuration menu 22.*

### 15.1 About SNMP

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



**Figure 15-1 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.

## 15.2 Supported MIBs

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

## 15.3 SNMP Configuration

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



```

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 15-2 Menu 22 SNMP Configuration**

The following table describes the SNMP configuration parameters.

**Table 15-1 Menu 22 SNMP Configuration**

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the <b>Get Community</b> , which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the <b>Set Community</b> , 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.		

## 15.4 SNMP Traps

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

**Table 15-2 SNMP Traps**

<b>TRAP #</b>	<b>TRAP NAME</b>	<b>DESCRIPTION</b>
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.

# Chapter 16

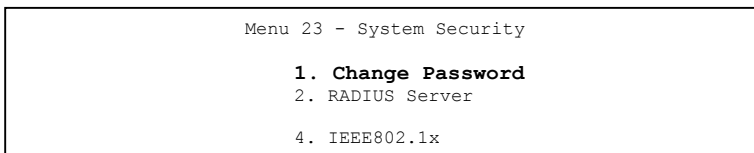
## System Security

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

### 16.1 System Security

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

#### 16.1.1 System Password

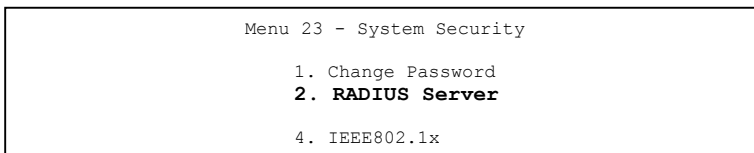


**Figure 16-1 Menu 23 System Security**

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.

#### 16.1.2 Configuring External RADIUS Server

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



**Figure 16-2 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 16-3 Menu 23.2 System Security : RADIUS Server**

The following table describes the fields in this menu.

**Table 16-1 Menu 23.2 System Security : RADIUS Server**

FIELD	DESCRIPTION	EXAMPLE
Authentication Server		
Active	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to enable user authentication through an external authentication server.	<b>No</b>
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 <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.	<b>1812</b>
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 <b>Yes</b> and press [ENTER] to enable user authentication through an external accounting server.	<b>No</b>
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	10.11.12.13

**Table 16-1 Menu 23.2 System Security : RADIUS Server**

FIELD	DESCRIPTION	EXAMPLE
Port	The default port of the RADIUS server for accounting is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.	<b>1813</b>
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points.  The key is not sent over the network. This key must be the same on the external accounting server and ZyAIR.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

### 16.1.3 802.1x

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

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

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

```

Menu 23 - System Security

1. Change Password
2. RADIUS Server

4. IEEE802.1X

```

**Figure 16-4 Menu 23 System Security**

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

```

Menu 23.4 - System Security - IEEE802.1x

Wireless Port Control= Authentication Required
ReAuthentication Timer (in second)= 1800
Idle Timeout (in second)= 3600

Key Management Protocol= 802.1x
Dynamic WEP Key Exchange= Disable
PSK = N/A
WPA Mixed Mode= N/A
Data Privacy for Broadcast/Multicast packets= N/A
WPA Broadcast/Multicast Key Update Timer= N/A

Authentication Databases= Local User Database Only

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

**Figure 16-5 Menu 23.4 System Security : IEEE802.1x**

The following table describes the fields in this menu.

**Table 16-2 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 <b>No Authentication Required</b> to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting.</p> <p>Selecting <b>Authentication Required</b> means wireless stations have to enter usernames and passwords before access to the wired network is allowed.</p> <p>Select <b>No Access Allowed</b> to block all wireless stations access to the wired network.</p> <p>The following fields are not available when you select <b>No Authentication Required</b> or <b>No Access Allowed</b>.</p>
ReAuthentic- ation Timer (in second)	<p>Specify how often a client has to re-enter username and password to stay connected to the wired network.</p> <p>This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is <b>1800</b> seconds (or 30 minutes).</p>

**Table 16-2 Menu 23.4 System Security : IEEE802.1x**

FIELD	DESCRIPTION
Idle Timeout (in second)	<p>The ZyAIR automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed.</p> <p>This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. The default time interval is <b>3600</b> seconds (or 1 hour).</p>
Key Management Protocol	<p>Press [SPACE BAR] to select <b>802.1x</b>, <b>WPA</b> or <b>WPA-PSK</b> and press [ENTER].</p>
Dynamic WEP Key Exchange	<p>This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Also set the <b>Authentication Databases</b> field to <b>RADIUS Only</b>. Local user database may not be used.</p> <p>Select <b>Disable</b> to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange.</p> <p>Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.</p> <p>Up to 32 stations can access the ZyAIR when you configure Dynamic WEP Key Exchange.</p>
PSK	<p>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select <b>WPA-PSK</b> in the <b>Key Management Protocol</b> field.</p>
WPA Mixed Mode	<p>Select <b>Enable</b> to activate WPA mixed mode. Otherwise, select <b>Disable</b> and configure <b>Data Privacy for Broadcast/Multicast packets</b> field.</p>
Data Privacy for Broadcast/Multicast packets	<p>This field allows you to choose <b>TKIP</b> (recommended) or <b>WEP</b> for broadcast and multicast ("group") traffic if the <b>Key Management Protocol</b> is <b>WPA</b> and <b>WPA Mixed Mode</b> is disabled. <b>WEP</b> is used automatically if you have enabled <b>WPA Mixed Mode</b>.</p> <p>All unicast traffic is automatically encrypted by <b>TKIP</b> when <b>WPA</b> or <b>WPA-PSK Key Management Protocol</b> is selected.</p>
WPA Broadcast/Multicast Key Update Timer	<p>The <b>WPA Broadcast/Multicast Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or RADIUS server (if using <b>WPA</b> key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Broadcast/Multicast Key Update Timer</b> is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).</p>

**Table 16-2 Menu 23.4 System Security : IEEE802.1x**

FIELD	DESCRIPTION
<p>Authentication Databases</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>When you configure <b>Key Management Protocol</b> to <b>WPA</b>, the <b>Authentication Databases</b> must be <b>RADIUS Only</b>. You can only use the <b>Local User Database</b> with <b>802.1x Key Management Protocol</b>.</p> <p>Select <b>Local User Database Only</b> 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 <b>RADIUS Only</b> 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 <b>Local first, then RADIUS</b> 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 <b>RADIUS first, then Local</b> 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>
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.</p>	

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



# Chapter 17

## System Information and Diagnosis

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

### 17.1 Overview

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
11. Remote Management Setup

Enter Menu Selection Number:
```

**Figure 17-1 Menu 24 System Maintenance**

### 17.2 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.

```

Menu 24.1 - System Maintenance - Status                                00:17:34
                                                                    Sat. Jan. 01, 2000

Port   Status      TxPkts    RxPkts    Cols    Tx B/s    Rx B/s    Up Time
ETH    100M/Full     164       690       0        273       128      0:12:33
WLAN   54M           629       1         0         0         0       0:12:53

Port   Ethernet Address      IP Address      IP Mask      DHCP
ETH    00:A0:C5:01:23:45     192.168.1.2    255.255.255.0  None
WLAN  00:A0:C5:01:23:45

System up Time:      0:12:59

Name: G-500
ZyNOS F/W Version: V3.50(HT.0)b3 | 03/12/2004

Press Command:
    
```

**Figure 17-2 Menu 24.1 System Maintenance : Status**

The following table describes the fields present in this menu.

**Table 17-1 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 ( <b>None</b> or <b>Client</b> ) for the port.

**Table 17-1 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.

## 17.3 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 17-3 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.**

### 17.3.1 System Information

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

```

Menu 24.2.1 - System Maintenance - Information

Name: G-500
Routing: BRIDGE
ZyNOS F/W Version: V3.50(HT.0)b3 | 03/12/2004
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 17-4 Menu 24.2.1 System Information : Information**

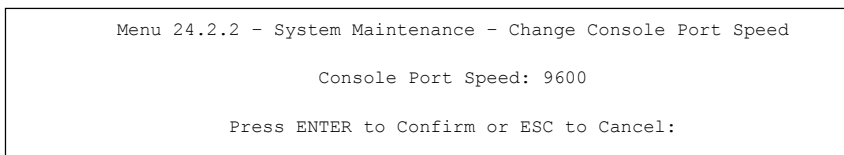
The following table describes the fields in this menu.

**Table 17-2 Menu 24.2.1 System Maintenance : Information**

FIELD	DESCRIPTION
Name	Displays the system name of your ZyAIR. This information can be changed in <b>Menu 1 – General Setup</b> .
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.	

### 17.3.2 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 17-5 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.

## 17.4 Log and Trace

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

### 17.4.1 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 17-6 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.

```

51 Sat Jan 1 00:00:00 2000 PINI INFO main: init completed
52 Sat Jan 1 00:00:02 2000 PP05 -WARN SNMP TRAP 3: link up
53 Sat Jan 1 00:00:30 2000 PSSV -WARN SNMP TRAP 0: cold start
54 Sat Jan 1 00:04:33 2000 PINI INFO SMT Session Begin
55 Sat Jan 1 00:04:39 2000 PINI -WARN SNMP TRAP 6: System reboot by user!
56 Sat Jan 1 00:04:39 2000 PP07 INFO LAN promiscuous mode <1>
57 Sat Jan 1 00:04:39 2000 PINI INFO Last errorlog repeat 1 Times
58 Sat Jan 1 00:04:39 2000 PINI INFO main: init completed
59 Sat Jan 1 00:04:41 2000 PP05 -WARN SNMP TRAP 3: link up
60 Sat Jan 1 00:05:09 2000 PSSV -WARN Last errorlog repeat 1 Times
61 Sat Jan 1 00:05:09 2000 PSSV -WARN SNMP TRAP 0: cold start
62 Sat Jan 1 00:06:11 2000 PP09 INFO SMT Password pass
63 Sat Jan 1 00:06:11 2000 PINI INFO SMT Session Begin

Clear Error Log (y/n):

```

**Figure 17-7 Sample Error and Information Messages**

## 17.5 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 17-8 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 17-3 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 18

## Firmware and Configuration File Maintenance

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

### 18.1 Filename Conventions

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

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

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

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

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

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

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

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

**Table 18-1 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.

## 18.2 Backup Configuration

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

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

### 18.2.1 Backup Configuration Using FTP

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

```

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 18-1 Menu 24.5 Backup Configuration**



## 18.2.2 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 18-2 FTP Session Example**

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

**Table 18-2 General Commands for Third Party FTP Clients**

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

**Table 18-2 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).

### 18.2.3 Backup Configuration Using TFTP

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

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

- 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.

### 18.2.4 Example: TFTP Command

The following is an example TFTP command:

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

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

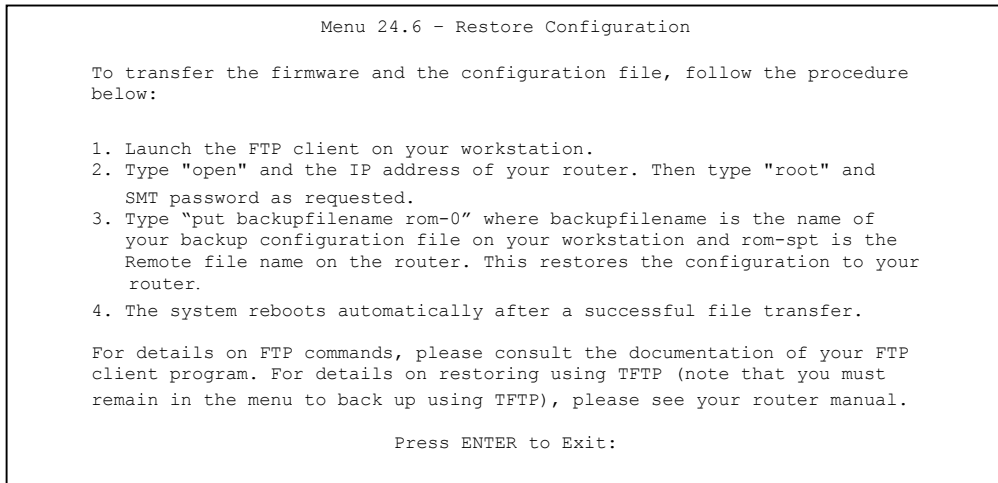
The following table describes some of the fields that you may see in third party TFTP clients.

**Table 18-3 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.

## 18.3 Restore Configuration

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

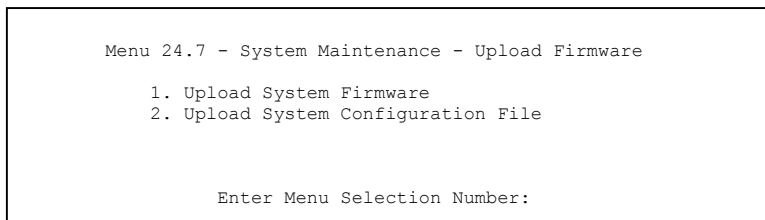


**Figure 18-3 Menu 24.6 Restore Configuration**

## 18.4 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.**



**Figure 18-4 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.

## 18.4.1 Firmware Upload

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

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

```
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.

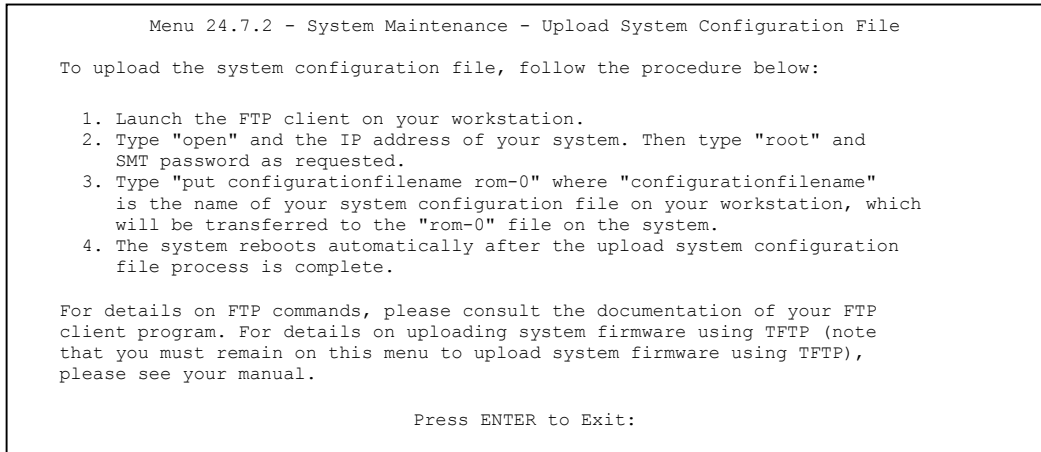
For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

**Figure 18-5 Menu 24.7.1 System Maintenance : Upload System Firmware**

## 18.4.2 Configuration File Upload

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



**Figure 18-6 Menu 24.7.2 System Maintenance : Upload System Configuration File**

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

### 18.4.3 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 18-7 FTP Session Example**

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

### 18.4.4 TFTP File Upload

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

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

- 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.

### 18.4.5 Example: TFTP Command

The following is an example TFTP command:

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

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

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



# Chapter 19

## System Maintenance and Information

*This chapter leads you through SMT menus 24.8 and 24.10.*

### 19.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the [zyxel.com](http://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
11. Remote Management Setup

Enter Menu Selection Number:
```

**Figure 19-1 Menu 24 System Maintenance**

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
G-500> ?
Valid commands are:
sys          exit          device          ether
config      wlan           ip              ppp
bridge      hdap          cnm             radius
8021x
G-500>
```

**Figure 19-2 Valid CI Commands**

## 19.2 Time and Date Setting

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

```
Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= NTP (RFC-1305)
Time Server Address= 128.105.39.21

Current Time:                05 : 47 : 19
New Time (hh:mm:ss):        05 : 47 : 17

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2000 - 01 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):         01 - 01
End Date (mm-dd):           01 - 01

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

**Figure 19-3 Menu 24.10 System Maintenance : Time and Date Setting**

The following table describes the fields in this menu.

**Table 19-1 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><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.</p> <p><b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p><b>NTP (RFC-1305)</b> is similar to <b>Time (RFC-868)</b>.</p> <p><b>None.</b> 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 <b>Yes</b> .
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.	

### 19.2.1 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.



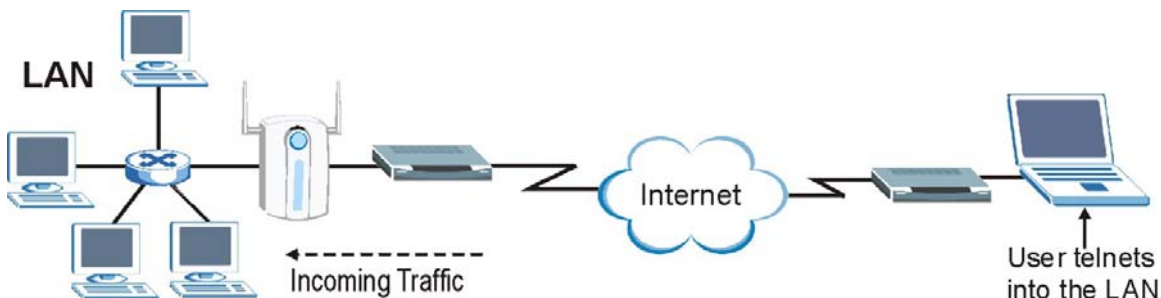
# Chapter 20

## Remote Management

*This chapter covers remote management (SMT menu 24.11).*

### 20.1 Telnet

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



**Figure 20-1 Telnet Configuration on a TCP/IP Network**

### 20.2 FTP

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

### 20.3 Web

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

### 20.4 Remote Management

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

Enter 11 from menu 24 to display **Menu 24.11 – Remote Management Control**.

## 20.4.1 Remote Management Setup

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

You may manage your ZyAIR from a remote location via:

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

- WLAN only
- ALL (LAN and WLAN)
- LAN only
- Disable (Neither)

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

```

Menu 24.11 - Remote Management Control

TELNET Server:      Port = 23           Access = ALL
                   Secured Client IP = 0.0.0.0

FTP Server:        Port = 21           Access = ALL
                   Secured Client IP = 0.0.0.0

Web Server:        Port = 80           Access = ALL
                   Secured Client IP = 0.0.0.0

SNMP Service:      Port = 161          Access = ALL
                   Secured Client IP = 0.0.0.0

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

**Figure 20-2 Menu 24.11 Remote Management Control**

The following table describes the fields in this menu.

**Table 20-1 Menu 24.11 Remote Management Control**

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service	Each of these read-only labels denotes a service or protocol.	
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the ZyAIR.  The DNS Service port number is 53. This cannot be changed.	

**Table 20-1 Menu 24.11 Remote Management Control**

FIELD	DESCRIPTION	EXAMPLE
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: <b>LAN only</b> , <b>WLAN only</b> , <b>All</b> or <b>Disable</b> . The default is <b>LAN only</b> .	LAN only
Secured Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the ZyAIR. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
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.		

## 20.4.2 Remote Management Limitations

Remote management over LAN or WLAN will not work when:

1. You have disabled that service in menu 24.11.
2. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

## 20.5 System Timeout

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





---

# Part VI:

---

## **APPENDICES**

---

This part provides troubleshooting and background information about setting up your computer's IP address, wireless LAN, 802.1x and IP subnetting. It also provides information on the command interpreter interface 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 <b>ETHN</b> LED on the front panel is off, check the Ethernet cable connection between your ZyAIR and the Ethernet device connected to the <b>ETHERNET</b> port.  Check for faulty Ethernet cables.  Make sure your computer's Ethernet adapter is installed and working properly.  Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of the 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 <b>ETHN</b> 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 <b>Password</b> and <b>Username</b> fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.</p> <p>Use the <b>RESET</b> 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**

<b>PROBLEM</b>	<b>CORRECTIVE ACTION</b>
Cannot access the ZyAIR from the WLAN.	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 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 pwderrtm</code>	This command displays the brute-force guessing password protection settings.
<code>sys pwderrtm 0</code>	This command turns off the password's protection from brute-force guessing.
<code>sys pwderrtm 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 pwderrtm 5` This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

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.

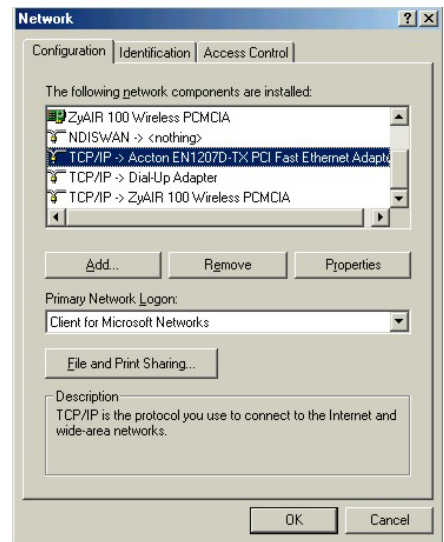
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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:

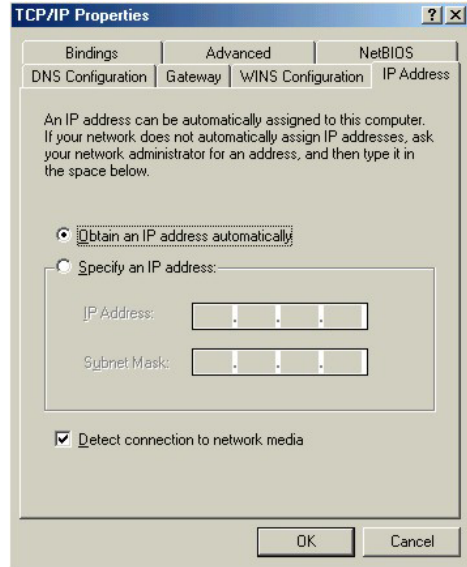
- a. Click **Add**.
- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

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**.

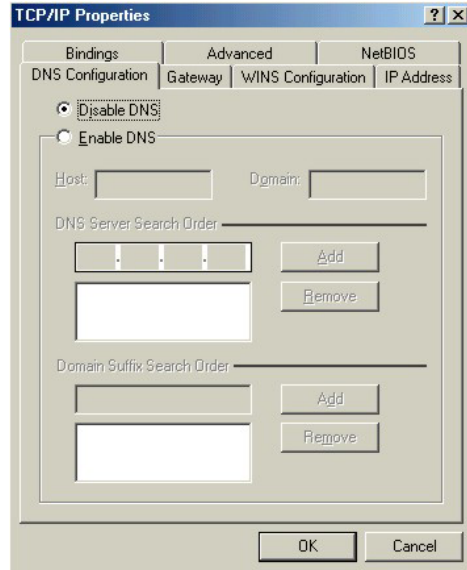
-If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



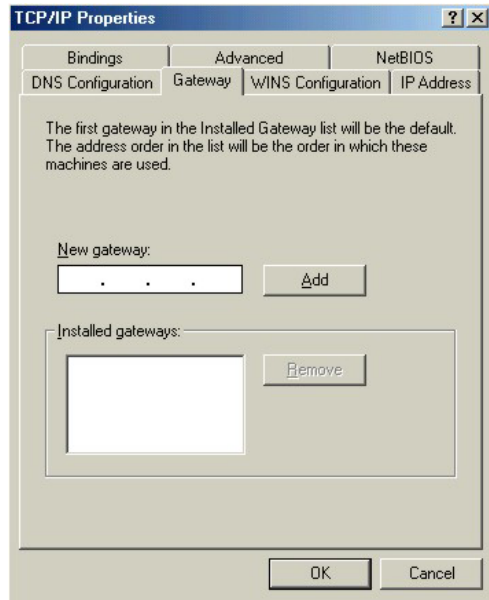
2. Click the **DNS Configuration** tab.

-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**.



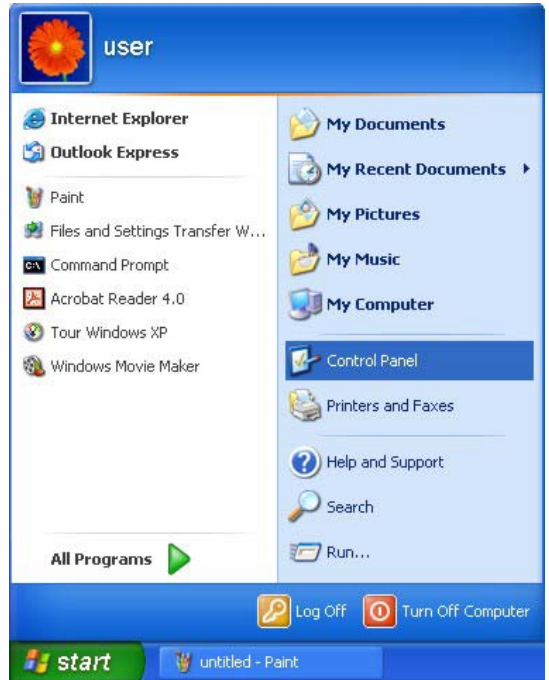
4. Click **OK** to save and close the **TCP/IP Properties** window.
5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
6. Turn on your ZyAIR and restart your computer when prompted.

### 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

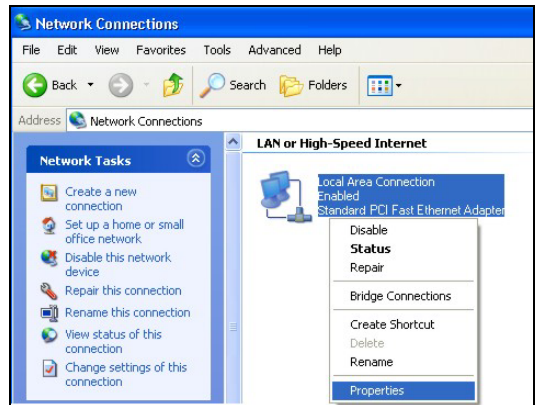
1. For Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.



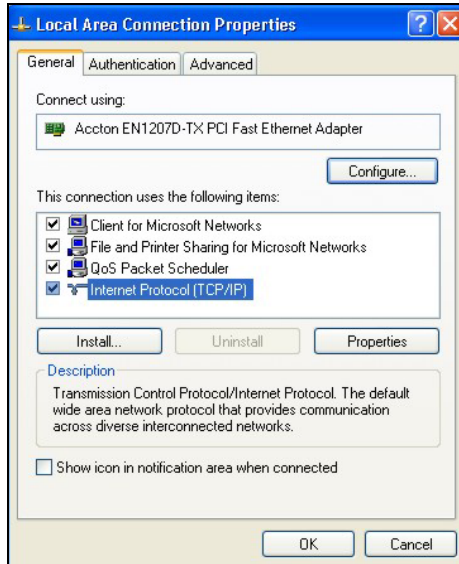
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



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**.

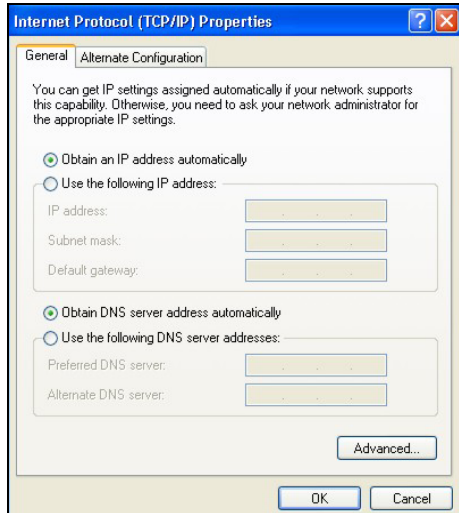


5. The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

-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.

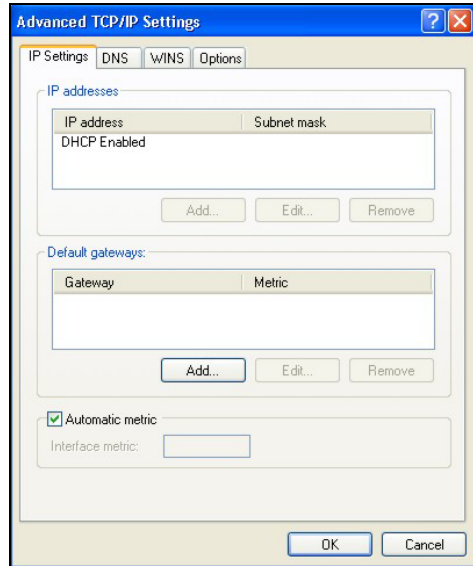
-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-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.

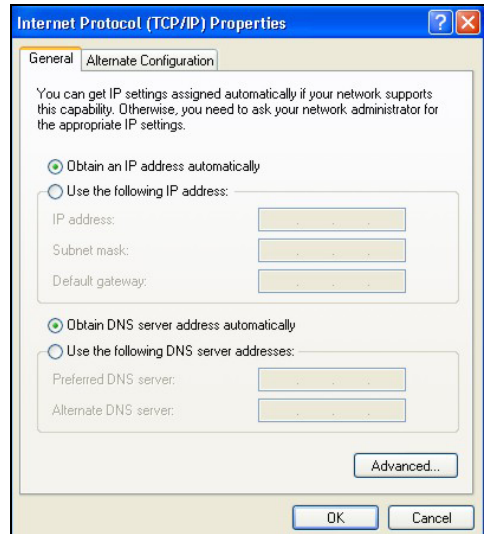


7. In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

-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).

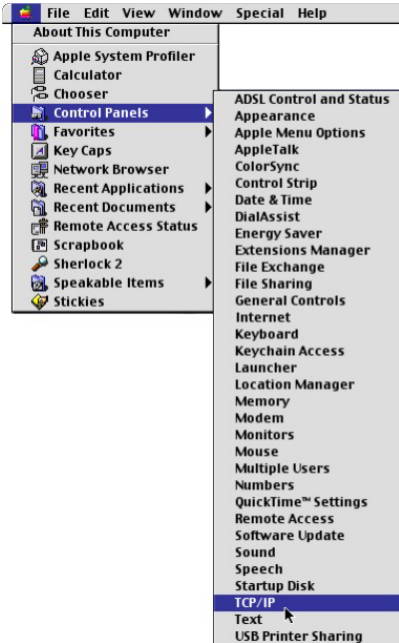
### Verifying Your Computer's IP Address

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.

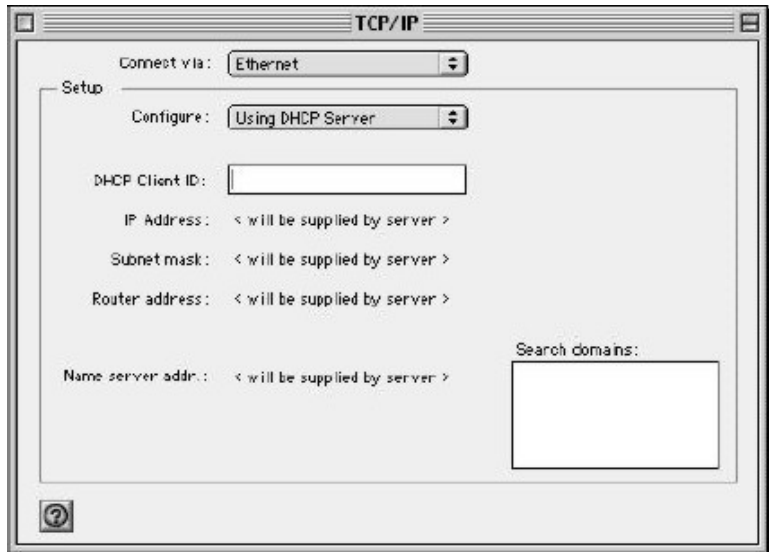
## Macintosh OS 8/9



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.

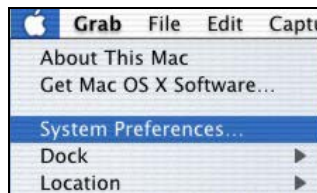
4. For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyAIR in the **Router address** box.
5. Close the **TCP/IP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

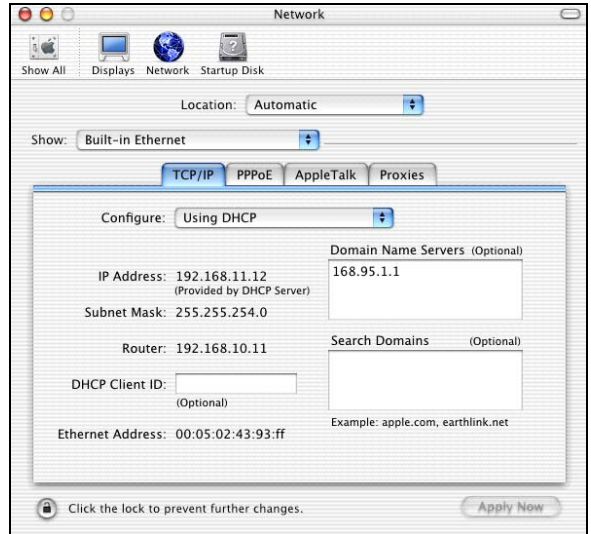
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

### 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

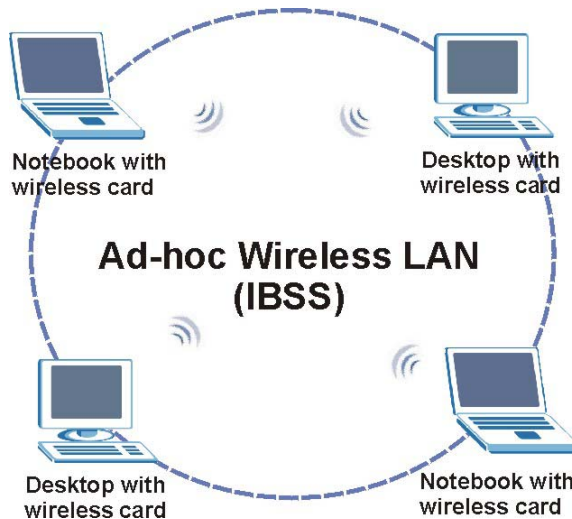
The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

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.

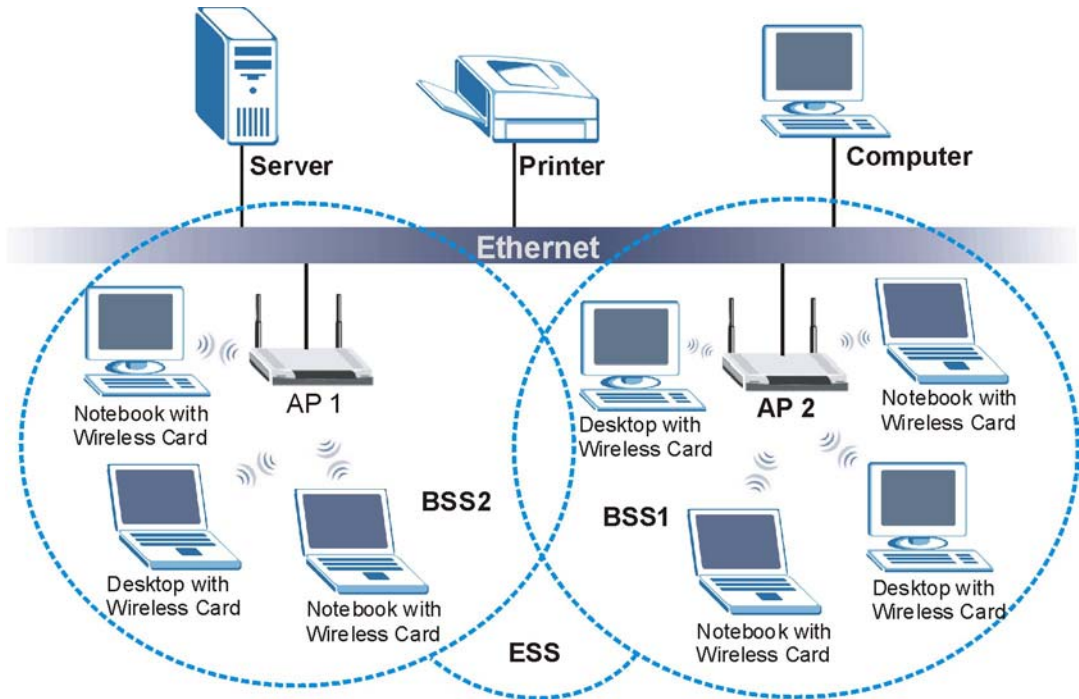


**Diagram D-1 Peer-to-Peer Communication in an Ad-hoc Network**

## 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

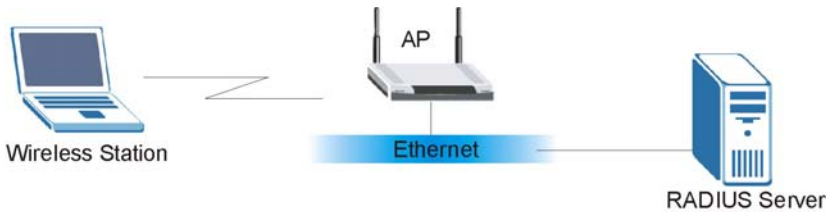
In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

### Advantages of the IEEE 802.1x

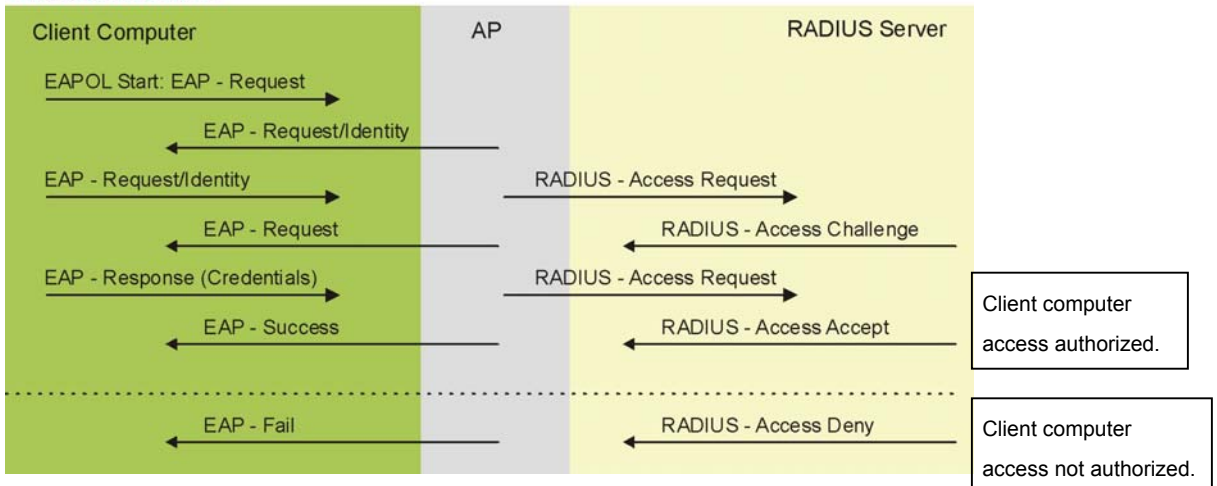
- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional 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).



**Unauthorized State**



**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**

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

# Appendix G

## 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 G-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 G-2 Allowed IP Address Range By Class**

<b>CLASS</b>	<b>ALLOWED RANGE OF FIRST OCTET (BINARY)</b>	<b>ALLOWED RANGE OF FIRST OCTET (DECIMAL)</b>
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 G-3 “Natural” Masks**

<b>CLASS</b>	<b>NATURAL MASK</b>
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 G-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 G-5 Subnet 1**

	<b>NETWORK NUMBER</b>	<b>LAST OCTET BIT VALUE</b>
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>
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 G-6 Subnet 2**

	<b>NETWORK NUMBER</b>	<b>LAST OCTET BIT VALUE</b>
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	<b>10000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>
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 G-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 G-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 G-9 Subnet 3**

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

**Chart G-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 G-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 G-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 G-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 G-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 G-13 Class B Subnet Planning**

<b>NO. "BORROWED" HOST BITS</b>	<b>SUBNET MASK</b>	<b>NO. SUBNETS</b>	<b>NO. HOSTS PER SUBNET</b>
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 H

## 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 [www.zyxel.com](http://www.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 I

## Log Descriptions

**Chart I-1 System Maintenance Logs**

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The ZyAIR has adjusted its time based on information from the time server.
Time calibration failed	The ZyAIR 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 ZyAIR 's SMT interface.
SMT Login Fail	Someone has failed to log on to the ZyAIR s SMT interface.
WEB Login Successfully	Someone has logged on to the ZyAIR 's web configurator interface.
WEB Login Fail	Someone has failed to log on to the ZyAIR 's web configurator interface.
TELNET Login Successfully	Someone has logged on to the ZyAIR via telnet.
TELNET Login Fail	Someone has failed to log on to the ZyAIR via telnet.
FTP Login Successfully	Someone has logged on to the ZyAIR via FTP.
FTP Login Fail	Someone has failed to log on to the ZyAIR via FTP.

**Chart I-2 ICMP Notes**

<b>TYPE</b>	<b>CODE</b>	<b>DESCRIPTION</b>
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
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



Chart I-2 ICMP Notes

TYPE	CODE	DESCRIPTION
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 I-3 Sys log

LOG MESSAGE	DESCRIPTION
<pre>Mon dd hr:mm:ss hostname src="&lt;srcIP:srcPort&gt;" dst="&lt;dstIP:dstPort&gt;" msg="&lt;msg&gt;" note="&lt;note&gt;"</pre>	This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts.

## Log Commands

Go to the command interpreter interface (the *Command Interpreter Appendix* explains how to access and use the commands).

### Configuring What You Want the ZyAIR to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyAIR is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

**Chart I-4 Log Categories and Available Settings**

LOG CATEGORIES	AVAILABLE PARAMETERS
8021x	0, 1
access	0, 1, 2, 3
error	0, 1, 2, 3
icmp	0, 1
mten	0, 1
packetfilter	0, 1
remote	0, 1
tcpreset	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 J

## Index

### A

Address Assignment.....	3-4
Ad-hoc Configuration.....	D-2
Alternative Subnet Mask Notation.....	G-3
Applications .....	1-3
auto-negotiation.....	1-1

### B

backup .....	18-2
Backup.....	10-8
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.....	G-1
Collision .....	17-2
Command Interpreter .....	19-1
Community.....	15-2
Computer's IP Address .....	C-1
Copyright.....	ii
CPU Load.....	17-3
Customer Support.....	v

### D

Data encryption .....	3-1
Default.....	10-10
DHCP .....	17-4
Diagnostic .....	17-6
Diagnostic Tools .....	17-1
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 .....	1-3, 6-1
EAP Authentication .....	F-1
MD5 .....	F-1
TLS.....	F-1
TTLS.....	F-1
Encryption .....	6-11
Error Log .....	17-5
Error/Information Messages	
Sample.....	17-5
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 .....	18-1
<i>Firmware File</i>	
<i>Maintenance</i> .....	10-4
Fragment Threshold.....	13-3
Fragmentation Threshold.....	5-4
Frequency-Hopping Spread Spectrum .....	D-2
FTP .....	8-1, 8-3, 20-3
Restrictions.....	20-3
FTP File Transfer.....	18-7
FTP Restrictions .....	8-1

### G

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

**H**

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

**I**

IBSS..... *See* Independent Basic Service Set  
 IEEE 802.11 .....D-1  
     Deployment Issues ..... E-1  
     Security Flaws..... E-1  
 IEEE 802.1x ..... E-1, 1-3  
     Advantages..... E-1  
 Independent Basic Service Set..... D-2, 5-1  
 Infrastructure Configuration .....D-2  
 Internet access.....13-1  
 Internet Access ..... 1-4, 1-5  
 Internet Security Gateway .....1-1  
 IP Address ..... 3-4, 3-5, 7-1, 13-2, 17-4, 17-6  
 IP Addressing .....G-1  
 IP Classes.....G-1

**L**

Link type.....17-2  
 Log and Trace.....17-5  
 Log Descriptions..... I-1  
 Logs.....9-1

**M**

MAC Address Filter Action..... 6-8, 13-7  
 MAC Address Filtering .....13-5  
 Main Menu .....11-4  
 Management Information Base (MIB)..... 8-6, 15-2  
 MD5 ..... F-1  
 Message Digest Algorithm 5 ..... *See* MD5  
 Message Integrity Check .....6-11  
 MIC ..... *See* Message Integrity Check

**N**

Network Management .....1-3  
 Network Topology With RADIUS Server ExampleE-2

**P**

Packets .....17-2  
 Password .....4-2, 11-1, 15-2  
 Ping .....17-6  
 Preamble Mode ..... 6-3  
 Private IP Address..... 3-5

**Q**

Quick Installation Guide ..... xvii

**R**

RADIUS..... 1-3  
 RAS.....17-4  
 Rate  
     Receiving.....17-2  
     Transmission.....17-2  
 Related Documentation..... xvii  
 Remote Authentication Dial In User Service ..... *See*  
     RADIUS  
 Remote Management ..... 8-1  
 Remote Management Limitations ..... 8-1, 20-3  
 Remote Management Setup .....20-1, 20-2  
 Remote Node .....17-2  
 Required fields .....11-4  
 Restore .....10-9  
 Restore Configuration .....18-5  
 RF signals ..... D-1  
 Roaming  
     Example.....5-7  
     Requirements.....5-8  
 RTS Threshold .....5-3, 13-3

**S**

Security Parameters..... 6-13  
 Server .....4-5  
 Service ..... iv  
 Service Set .....5-6  
 SMT Menu Overview .....11-2  
 SNMP .....8-5  
     Community .....15-3  
     Configuration.....15-2  
     Get .....8-6, 15-2

GetNext.....	15-2
Manager.....	8-6, 15-2
MIBs.....	8-7, 15-2
Set.....	15-2
Trap.....	8-7, 15-2
Traps.....	15-3, 15-4
Trusted Host.....	15-3
SNMP Traps.....	8-7
Subnet Mask.....	3-5, 7-1, 13-2, 17-4
Subnet Masks.....	G-2
Subnetting.....	G-3
Supporting Disk.....	xvii
System	
Console Port Speed.....	17-4
Diagnostic.....	17-6
Log and Trace.....	17-5
System Information.....	17-3
System Status.....	17-1
Time and Date.....	19-2
System Information.....	17-3
System Information & Diagnosis.....	17-1
System Maintenance..	17-1, 17-3, 18-2, 18-4, 18-5, 18-6, 18-9, 19-1, 19-2, 19-3
System Management Terminal.....	11-4
System Name.....	4-2
System Timeout.....	8-1, 20-3

**T**

TCP/IP.....	8-2, 17-6, 20-1
Telnet.....	8-2, 20-1
Telnet Configuration.....	8-2, 20-1
Telnet Under NAT.....	20-1
Temporal Key Integrity Protocol.....	6-11
TFTP	
And FTP Over WAN}.....	20-3
Restrictions.....	20-3
TFTP and FTP Over WAN}.....	8-1
TFTP File Transfer.....	18-9
TFTP Restrictions.....	8-1
Time and Date Setting.....	19-2
Time Server.....	19-3
Time Zone.....	19-3
TKIP.....	<i>See</i> Temporal Key Integrity Protocol
TLS.....	F-1

Trace Records.....	17-5
Transport Layer Security.....	<i>See</i> 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.....	<i>See</i> TTLS

**U**

Upload Firmware.....	18-6
User Authentication.....	6-11
User Profiles.....	6-21, 14-1

**V**

Valid CI Commands.....	19-1
------------------------	------

**W**

Web.....	8-4
Web Configurator.....	2-1, 2-3
WEP.....	3-1
WEP Encryption.....	6-5, 13-3
Wi-Fi Protected Access.....	1-2
Wireless Client WPA Supplicants.....	6-14
Wireless LAN.....	D-1, 13-2
Benefits.....	D-1
Wireless LAN Setup.....	13-2
Wizard Setup.....	3-1, 3-2, 3-3, 3-4
WLAN.....	<i>See</i> Wireless LAN
WPA.....	6-11
WPA with RADIUS Application.....	6-12
WPA-PSK.....	6-11
WPA-PSK Application.....	6-12

**Z**

ZyNOS.....	18-1, 18-2
ZyNOS F/W Version.....	18-1
ZyXEL Limited Warranty	
Note.....	iv

