ZyAIR B-4000

Hot Spot Gateway

User's Guide

Version 1.04

March 2004

ZyXEL

Unleash Networking Power

Copyright

Disclaimer

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

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

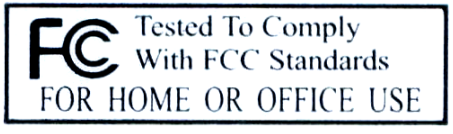
1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Certifications

1. Go to 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 lightening.

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[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
CZECH REPUBLIC	info@cz.zyxel.com info@cz.zyxel.com	+420 241 091 350 +420 241 091 359	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 – Modrany Ceská Republika
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.

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

METHOD / LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
UNITED KINGDOM	support@zyxel.co.uk sales@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only) +44 (0) 1344 303034	www.zyxel.co.uk ftp.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

Table of Contents

Copyright ..... **ii**
Federal Communications Commission (FCC) Interference Statement ..... **iii**
ZyXEL Limited Warranty ..... **iv**
Customer Support ..... **v**
List of Figures ..... **xiii**
List of Tables ..... **xvii**
Preface ..... **xix**
Getting Started ..... **I**
Chapter 1 Getting to Know Your ZyAIR **1-1**
1.1 Introducing the ZyAIR 1-1
1.2 Features 1-1
1.3 Applications 1-5
1.3.1 Internet Access for LAN Networks 1-5
1.3.2 Internet Access in Public Areas 1-5
Chapter 2 The Web Configurator **2-1**
2.1 Introducing the Web Configurator 2-1
2.2 Accessing the Web Configurator 2-1
2.3 Wizard Setup Screens 2-2
2.4 Navigating the Web Configurator 2-2
2.5 Screens Overview 2-4
2.6 Login Accounts 2-8
2.6.1 Changing Login Account Usernames and Passwords 2-8
2.7 Methods of Restoring Factory-Defaults 2-10
2.7.1 Using the Reset Button to Restore Factory-Defaults 2-11
2.7.2 Using the Web Configurator to Restore Factory-Defaults 2-11
2.8 Restarting the ZyAIR 2-13
2.9 Logging Out of the Web Configurator 2-13
Chapter 3 General System Setup **3-1**
3.1 General System Settings 3-1
Chapter 4 WAN, LAN and Server Setup **4-1**
4.1 Factory Ethernet Defaults 4-1
4.2 LANs and WANs 4-1
4.3 IP Address Assignment 4-1
4.4 DHCP Configuration 4-1
4.4.1 IP Address and Subnet Mask 4-2
4.4.2 Private IP Addresses 4-2
4.5 DNS Server Address 4-2
4.6 PPPoE 4-3

4.6.1 PPP MTU 4-3
4.6.2 TCP MSS 4-3
4.7 PPTP 4-4
4.8 Configuring the WAN and LAN Settings 4-4
4.9 Server Configuration 4-7
Subscriber Account Management II
Chapter 5 Authentication 5-1
5.1 About the Built-in Authentication 5-1
5.2 Authentication Settings 5-1
Chapter 6 Billing 6-1
6.1 About the Built-in Billing 6-1
6.1.1 Accumulation Accounting Method 6-1
6.1.2 Time-to-finish Accounting Method 6-1
6.2 Billing Settings 6-1
Chapter 7 Accounting 7-1
7.1 About Subscriber Accounts 7-1
7.2 Discount Price Plan 7-1
7.2.1 Charge By Levels 7-1
7.3 Accounting Settings 7-1
7.3.1 Charge By Levels Example 7-5
7.4 Creating Accounts 7-6
7.4.1 Creating Accounts in the Web Configurator 7-6
7.4.2 Using the Exclusive Printer to Create and Print Subscriber Statements 7-8
7.5 Viewing the Account List 7-9
Chapter 8 Credit Card 8-1
8.1 About the Credit Card Screen 8-1
8.2 Credit Card Settings 8-1
Advanced Subscriber Account Management III
Chapter 9 Keypad 9-1
9.1 About the Keypad 9-1
9.2 Keypad Settings 9-1
9.3 Keypad Configuration Examples 9-3
9.3.1 Keypad with Pre-Paid Billing Example 9-3
9.3.2 Keypad with Post-Paid Billing Example 9-5
Chapter 10 Customization 10-1
10.1 About the Customization Screens 10-1
10.2 About the Login Page Screen 10-1
10.3 Customizing the Subscriber Login Screen 10-1
10.3.1 Standard Subscriber Login Screen 10-3
10.3.2 Redirect Subscriber Login Screen 10-4
10.3.3 Advanced Subscriber Login Screen 10-5

10.3.4 Framed Subscriber Login Screen 10-8
10.4 Adding a Logo 10-9
10.5 About the Information Window 10-10
10.5.1 Customizing the Information Window 10-11
10.6 About the Account Printout 10-12
10.6.1 Customizing the Account Printout 10-12
10.7 Customizing the Credit Card 10-17
10.7.1 Credit Card Standard Login Page 10-17
10.7.2 Credit Card Service Selection Page 10-18
10.7.3 Credit Card Successful Page 10-22
10.7.4 Credit Card Fail Page 10-25
Chapter 11 Pass Through 11-1
11.1 About the Pass Through 11-1
11.2 Configuring Pass Through 11-1
Chapter 12 Filtering 12-1
12.1 About Filtering 12-1
12.2 Configuring Filtering 12-1
Chapter 13 Share 13-1
13.1 About Share 13-1
13.2 Configuring Share 13-1
Advanced Subscriber Account Management 2 IV
Chapter 14 Portal Page, Advertisement Links and Walled Garden 14-1
14.1 Portal Page Advertisement Links and Walled Garden Overview 14-1
14.2 Portal Page 14-1
14.3 Advertisement Links 14-2
14.4 Walled Garden 14-3
14.4.1 Walled Garden Login Example 14-5
Chapter 15 DDNS 15-1
15.1 About DDNS 15-1
15.1.1 DYNDNS Wildcard 15-1
15.2 Configuring DDNS 15-1
Chapter 16 LAN Devices 16-1
16.1 LAN Devices and NAT Overview 16-1
16.1.1 Port Mapping 16-1
16.2 Configuring LAN Devices Port Mapping 16-1
16.2.1 LAN Device Management Example 16-3
16.2.2 Specifying an Inside Server Example 16-5
Chapter 17 Syslog 17-1
17.1 Syslog Configuration 17-1
17.2 Syslog Log Settings Configuration 17-3
Chapter 18 Wireless LAN 18-1

18.1 Wireless LAN Overview 18-1
18.1.1 IBSS 18-1
18.1.2 BSS 18-1
18.1.3 ESS 18-2
18.2 Wireless LAN Basics 18-3
18.2.1 Channel 18-3
18.2.2 WEP Encryption 18-3
18.2.3 RTS/CTS 18-3
18.2.4 Fragmentation Threshold 18-5
18.2.5 Preamble Type 18-5
18.3 Wireless LAN Setup 18-5
18.3.1 Configuring WEP Keys 18-8
System Status, System Tools and Troubleshooting V
Chapter 19 System Status 19-1
19.1 About System Status 19-1
19.2 View System Information 19-1
19.3 Account List 19-5
19.4 Account Log 19-5
19.5 Current Users 19-7
19.6 DHCP Clients 19-8
19.7 Session List 19-9
19.8 LAN Devices 19-10
19.8.1 Accessing a LAN Device 19-11
Chapter 20 Configuration, Firmware and Accounting Log Maintenance 20-1
20.1 Filename Conventions 20-1
20.2 Configuration File Maintenance 20-1
20.2.1 Backup Configuration Using HTTP 20-1
20.2.2 Backup Configuration Using TFTP 20-3
20.2.3 Restore Configuration Using HTTP 20-5
20.2.4 Restore Configuration Using TFTP 20-6
20.3 Firmware Upgrade 20-7
20.3.1 Manual Firmware Upgrade Using the Web Configurator 20-7
20.3.2 Manual Firmware Upgrade via TFTP Server 20-8
20.3.3 Scheduled Firmware Upgrade 20-9
Chapter 21 SSL (Secure Socket Layer) Security 21-1
21.1 About SSL 21-1
21.2 Activating SSL Security for Management Connections 21-1
21.3 Viewing and Installing the SSL Security Certificate 21-2
21.4 Activating SSL Security for Subscriber Logins 21-8
21.5 SSL Certificate Download 21-9
Chapter 22 Ping Command 22-1

22.1 About Ping Command....22-1
22.2 Using Ping Command....22-1
Chapter 23 Troubleshooting....23-1
23.1 Using LEDs to Diagnose Problems....23-1
23.1.1 The Power LED....23-1
23.1.2 The LAN Port LEDs....23-1
23.1.3 The WAN Port LED....23-1
23.2 Web Configurator....23-2
23.3 Internet Access....23-3
23.4 The Statement Printer....23-3
Additional Information....VI
Appendix A Setting up Your Computer's IP Address....A-1
Appendix B IP Address Assignment Conflicts....B-1
Appendix C Wireless LAN and IEEE 802.11....C-1
Appendix D Antenna Selection and Positioning Recommendation....D-1
Appendix E PPPoE....E-1
Appendix F PPTP....F-1
Appendix G IP Subnetting....G-1
Appendix H Subscriber Login....H-1
Appendix I Cable Types and Cable Pin Assignments....I-1
Appendix J Index....J-1

List of Figures

Figure 1-1 Application: Internet Access for LAN Networks 1-5
Figure 1-2 Application: Internet Access in Public Areas 1-6
Figure 2-1 Entering ZyAIR IP Address in Internet Explorer 2-1
Figure 2-2 Web Configurator: Login 2-2
Figure 2-3 Web Configurator Navigation 2-3
Figure 4 WIZARD Submenu 2-4
Figure 5 Quick View 2-6
Figure 2-6 SYSTEM TOOLS: SYSTEM ACCOUNT 2-9
Figure 2-7 Side Panel 2-11
Figure 2-8 Reset to Default Settings 2-12
Figure 2-9 Restart 2-13
Figure 2-10 Logging Out 2-13
Figure 3-1 SYSTEM 3-2
Figure 4-1 WAN/LAN 4-5
Figure 4-2 SERVER 4-8
Figure 5-1 AUTHENTICATION 5-1
Figure 6-1 BILLING 6-2
Figure 7-1 ACCOUNTING 7-2
Figure 7-2 Charge By Levels Example 7-5
Figure 7-3 Account Generator Panel 7-6
Figure 7-4 Web-based Account Generator Printout Preview Example 7-7
Figure 7-5 Web-based PC-connected Printout Preview Example 7-8
Figure 7-6 Account List 7-9
Figure 8-1 CREDIT CARD 8-2
Figure 9-1 KEYPAD 9-2
Figure 9-2 Select Pre-Paid Billing 9-4
Figure 9-3 Define Pre-Paid Billing Profiles 9-4
Figure 9-4 Billing Profiles 1 and 2 Examples 9-5
Figure 9-5 Select Post-Paid Billing 9-6
Figure 9-6 Define Post-Paid Billing Plan 9-7
Figure 9-7 Post-Paid Account Printout Example 9-8
Figure 9-8 Post-Paid Account Bill Printout Example 9-9
Figure 10-1 Login Page 10-2
Figure 10-2 Login Page: Standard 10-3
Figure 10-3 Login Page Example: Standard 10-4
Figure 10-4 Login Page: Redirect 10-4
Figure 10-5 Login Page: Redirect Code 10-5

Figure 10-6 Login Page: Advanced 10-6
Figure 10-7 Login Page: Color Grid 10-7
Figure 10-8 Subscriber Login Screen Example: Advanced 10-8
Figure 10-9 Subscriber Login Screen: Frame 10-8
Figure 10-10 Subscriber Login Screen Example: Frame 10-9
Figure 10-11 Logo 10-10
Figure 10-12 Customization: Information Window 10-11
Figure 10-13 Account Printout 10-13
Figure 10-14 Preview of PC-connected Printer Example 10-15
Figure 10-15 Preview of Account Generator Printer Example 10-16
Figure 10-16 Preview of Post-Paid Printout Example 10-17
Figure 10-17 Credit Card: Standard Login Page 10-18
Figure 10-18 Credit Card Standard Login Page Example 10-18
Figure 10-19 Credit Card Service Selection Page 10-19
Figure 10-20 Credit Card Service Selection Page Preview 10-22
Figure 10-21 Credit Card Successful Page 10-23
Figure 10-22 Credit Card Successful Page Preview 10-24
Figure 10-23 Credit Card Service Fail Page 10-25
Figure 10-24 Credit Card Failed Page Preview 10-26
Figure 11-1 PASS THROUGH 11-2
Figure 12-1 FILTERING 12-2
Figure 13-1 SHARE 13-2
Figure 14-1PORTAL PAGE 14-1
Figure 14-2 ADVERTISEMENT 14-2
Figure 14-3 WALLED GARDEN 14-4
Figure 14-4 Walled Garden Login Example 14-5
Figure 15-1 DDNS 15-2
Figure 16-1 LAN DEVICES 16-2
Figure 16-2 LAN Device Remote Management Example 1 16-4
Figure 16-3 LAN Devices: Example 1 16-4
Figure 16-4 LAN Device Remote Management Example 2 16-5
Figure 16-5 LAN Devices: Example 2 16-5
Figure 17-1 Syslog 17-1
Figure 2 Log Settings 17-4
Figure 18-1 IBSS (Ad-hoc) Wireless LAN 18-1
Figure 18-2 Basic Service set 18-2
Figure 18-3 Extended Service Set 18-2
Figure 18-4 RTS/CTS 18-4
Figure 18-5 WIRELESS 18-6
Figure 18-6 WEP Key Setup 18-9
Figure 19-1 SYSTEM 19-2

Figure 19-2 ACCOUNT LOG 19-6
Figure 19-3 CURRENT USER 19-7
Figure 19-4 DHCP CLIENTS 19-8
Figure 19-5 SESSION LIST 19-9
Figure 19-6 LAN DEVICES 19-11
Figure 20-1 CONFIGURATION: Backup Using HTTP 20-2
Figure 2 Configuration Backup: File Download 20-3
Figure 20-3 Configuration Backup: Save As 20-3
Figure 20-4 CONFIGURATION: Backup using TFTP 20-4
Figure 20-5 Configuration Backup: Using TFTP Successful 20-4
Figure 20-6 CONFIGURATION: Restore Using HTTP 20-5
Figure 20-7 CONFIGURATION: Restore Using TFTP 20-6
Figure 20-8 Manual Firmware Upgrade Using the Web Configurator 20-7
Figure 20-9 System Restart 20-8
Figure 10 Manual Firmware Upgrade via TFTP Server 20-9
Figure 20-11 Scheduled Firmware Upgrade 20-10
Figure 20-12 Synchronization Check File Example 20-11
Figure 21-1 System Settings: Server Configuration: Enable SSL Security 21-2
Figure 21-2 Installing the SSL Security Certificate: First Security Alert 21-3
Figure 21-3 Installing the SSL Security Certificate: Second Security Alert 21-3
Figure 21-4 Installing the SSL Security Certificate: View Certificate 21-4
Figure 21-5 Installing the SSL Security Certificate: Certificate Import Wizard 21-5
Figure 21-6 Certificate Import Wizard: Location 21-5
Figure 21-7 Certificate Import Wizard: Finish 21-6
Figure 21-8 Root Certificate Store 21-6
Figure 21-9 Certificate Import Wizard 21-7
Figure 21-10 Certificate: Details 21-7
Figure 21-11 Security Alert: Trusted 21-8
Figure 21-12 AUTHENTICATION: Activate SSL Login 21-9
Figure 21-13 SSL CERTIFICATE 21-10

List of Tables

Table 1-1802.11B....1-3
Table 1-2 ZyAIR Wireless LAN Coverage....1-4
Table 2-1 Web Configurator Screens Overview....2-4
Table 2-2 Quick View....2-6
Table 2-3 SYSTEM TOOLS: SYSTEM ACCOUNT....2-10
Table 2-4 Reset to Default Settings....2-12
Table 3-1 SYSTEM....3-3
Table 4-1 WAN/LAN....4-6
Table 4-2 SERVER....4-9
Table 5-1 AUTHENTICATION....5-2
Table 6-1 BILLING....6-3
Table 7-1 ACCOUNTING....7-3
Table 7-2 Charge By Levels Example....7-6
Table 7-3 Account List....7-9
Table 8-1 CREDIT CARD....8-2
Table 9-1 KEYPAD....9-3
Table 10-1 Login Page: Standard....10-3
Table 10-2 Login Page: Redirect....10-4
Table 10-3 Login Page: Advanced....10-6
Table 10-4 Subscriber Login Screen: Frame....10-9
Table 10-5 Logo....10-10
Table 10-6 Customization: Information Window....10-12
Table 10-7 Account Printout....10-13
Table 10-8 Credit Card: Standard Login Page....10-18
Table 10-9 Credit Card Service Selection Page....10-20
Table 10-10 Credit Card Successful Page....10-23
Table 10-11 Credit Card Service Fail Page....10-25
Table 11-1 PASS THROUGH....11-2
Table 12-1 FILTERING....12-2
Table 13-1 SHARE....13-2
Table 14-1PORTAL PAGE....14-2
Table 14-2 ADVERTISEMENT....14-3
Table 14-3 WALLED GARDEN....14-4
Table 15-1 DDNS....15-3
Table 16-1 LAN DEVICES....16-2
Table 17-1 Syslog....17-2
Table 17-2 Log Settings....17-5

Table 17-3 Log Formats 17-5
Table 18-1 WIRELESS 18-7
Table 18-2 WEP Key Setup 18-9
Table 19-1 System 19-3
Table 2 ACCOUNT LOG 19-6
Table 19-3 CURRENT USER 19-8
Table 19-4 DHCP CLIENTS 19-8
Table 19-5 SESSION LIST 19-10
Table 19-6 LAN DEVICES 19-11
Table 20-1 Scheduled Firmware Upgrade 20-10
Table 21-1 SSL CERTIFICATE 21-10
Table 22-1 PING COMMAND 22-2
Table 23-1 Troubleshooting Power LED 23-1
Table 23-2 Troubleshooting LAN LEDs 23-1
Table 23-3 Troubleshooting WAN LEDs 23-2
Table 23-4 Troubleshooting the Web Configurator 23-2
Table 23-5 Troubleshooting the Internet Browser Display 23-3
Table 23-6 Troubleshooting Internet Access 23-3
Table 23-7 Troubleshooting the Statement Printer 23-4

Preface

Congratulations on your purchase of the ZyXEL ZyAIR B-4000 Hot Spot Gateway.

The ZyAIR Hot Spot Gateway combines an 802.11b wireless access point, router, 4-port switch and service gateway in one box. An "exclusive printer" connects directly to the ZyAIR, allowing you to easily print subscriber statements. The ZyAIR is ideal for offices, coffee shops, libraries, hotels and airport terminals catering to subscribers that seek Internet access. You should have an Internet account already set up and have been given usernames, passwords etc. required for Internet access.

This user's guide is designed to guide you through the configuration of your ZyAIR using the web configurator.

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

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Installation Guide

  The Quick Installation Guide is designed to help you get up and running right away. It contains information on the hardware connections and installation.

- ZyXEL Web Site

  The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

User Guide Feedback

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

Syntax Conventions

- "Enter" means for you to type one or more characters (and press the carriage return). "Select" or "Choose" means for you to use one of the predefined choices.
- 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 ZyXEL ZyAIR B-4000 Hot Spot Gateway may be referred to as the "ZyAIR" in this manual.
- The ZyXEL ZyAIR SP-200 Statement Printer may be referred to as the "statement printer" or the "exclusive printer" in this manual.

Part I:

Getting Started

This part introduces the ZyAIR, the web configurator and general system setup.

Chapter 1
Getting to Know Your ZyAIR

This chapter introduces the features and applications of the ZyAIR.

1.1 Introducing the ZyAIR

The ZyAIR Hot Spot Gateway combines an 802.11b wireless access point, router, 4-port switch and service gateway in one box. An "exclusive printer" connects directly to the ZyAIR, allowing you to easily print subscriber statements. The ZyAIR is ideal for offices, coffee shops, libraries, hotels and airport terminals catering to subscribers that seek Internet access. You should have an Internet account already set up and have been given usernames, passwords etc. required for Internet access.

1.2 Features

Your ZyAIR provides the following features to accommodate subscribers with a variety of network configurations with little or no technical support.

Plug-and-Play Internet Access

The ZyAIR provides Internet access to attached computer(s) without extra software installation or computer configuration. In addition, with transparent proxy, the ZyAIR resolves any incompatible proxy settings.

WEP Data Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private. The ZyAIR supports 64, 128 and 256-bit WEP encryption.

VPN (Virtual Private Network) Pass Through

The ZyAIR allows subscribers to create VPN networks (which use data encryption and the Internet to provide secure communications) that go through the ZyAIR.

VLAN

The ZyAIR can use VLANs (Virtual Local Area Network) to partition the physical network into multiple logical networks in order to stop subscribers from seeing each other's data. The ZyAIR also provides a port-based VLAN via the four 10/100Mbps auto-negotiating Ethernet ports.

SSL Secure Login

With Secure Socket Layer (SSL) activated upon login, data exchanged between the ZyAIR and client computers are encrypted and protected.

PPTP Support

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. Use PPTP to connect to a broadband modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

PPPoE Support (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the ZyAIR is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translations of multiple IP addresses used within one network to different IP addresses known within another network.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual computers (DHCP clients) to obtain TCP/IP configuration at start-up from a centralized DHCP server. The ZyAIR has built-in DHCP server capability. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The ZyAIR can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the DHCP clients.

E-mail Forwarding

The ZyAIR is able to forward and retrieve e-mail messages when the subscriber’s default email server is down or behind a firewall.

DNS Proxy

With DNS proxy, the ZyAIR provides DNS redirection when a subscriber’s configured DNS server is behind a firewall or located in a private Intranet.

Local Subscriber Database

The ZyAIR allows you to maintain a subscriber database on the ZyAIR without setting up an external RADIUS server. Subscriber accounting and authentication are done using the local subscriber database.

Accounting

Accounting can be done using the built-in accounting feature.

Local Content and Advertising Links

Once connected to the network, the ZyAIR directs the subscriber to a specified web site and display advertisement links. This can be a source of extra online advertising revenues and increased business exposure.

Access Control (Walled Garden)

With the walled garden feature, subscribers are able to access predetermined web sites without logging in. The ZyAIR blocks full Internet access until the subscribers log in.

Subscriber Login Page Customization

You can customize the subscriber login page according to your business needs. The advanced settings allow you to include welcome messages, company logo and basic formatting.

Web Configurator Management

The ZyAIR comes with an embedded web-based configurator. It offers advanced management features and allows you to manage the ZyAIR remotely using Internet Explorer.

Watchdog

The ZyAIR can continue working by resetting itself after a system crash.

Upgrade Firmware

The firmware of the ZyAIR can be upgraded via the web configurator.

Syslog

The ZyAIR's syslog function allows network administrators to monitor the usage status of subscribers from a remote site. You can set up a syslog server to receive the log of information on current logged-in subscribers that the ZyAIR sends periodically.

802.11b Wireless LAN Standard

The ZyAIR complies with the 802.11b wireless standard.

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

Table 1-1802.11B

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

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

Antennas

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

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

Table 1-2 ZyAIR Wireless LAN Coverage

	≤11 Mbps	≤ 5.5 Mbps
Indoor	50 m	80 m
Outdoor	200 m	300 m

4-Port Switch

A combination of switch and Internet gateway makes your ZyAIR a cost-effective and viable network solution. You can connect up to four computers to the LAN ports on the ZyAIR without the cost of a hub. To connect more than four Ethernet devices, attach a hub or switch.

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.

Reset Button

Use the reset button to restore the ZyAIR back to its factory defaults.

Statement Printer

A compact statement printer comes with your ZyAIR. The statement printer allows you to generate subscriber accounts on the ZyAIR and print out the account information on-site without using a computer.

The statement printer is also known as an "account generator" or "exclusive printer".

Ease of Installation

Your ZyAIR is designed for quick, intuitive and easy installation. It can be mounted on a desktop or a wall.

1.3 Applications

The following sections describe network application examples in which the ZyAIR is used. [1]

1.3.1 Internet Access for LAN Networks

With a broadband service account set up, the ZyAIR allows the attached computers to enjoy high speed Internet access.

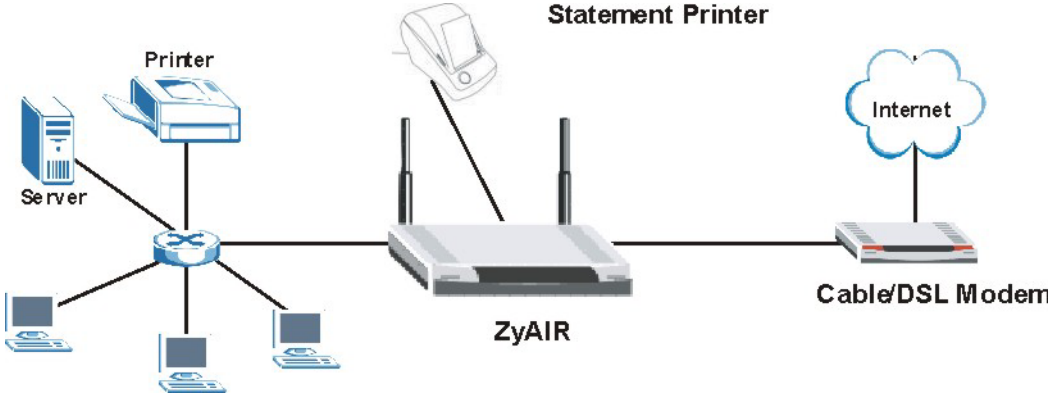


Figure 1-1 Application: Internet Access for LAN Networks

1.3.2 Internet Access in Public Areas

In public areas, such as a hotel, the ZyAIR provides high speed Internet access to subscribers. Account billing and authentication can be done using the built-in billing function and local subscriber database.

The ZyAIR functions as an access point (AP) to bridge the wired and the wireless network allowing wireless stations to access the Internet through the ZyAIR.

[1] The total number of concurrent WLAN users allowed is 24. The total number of concurrent users (WLAN and Wired) allowed is 100

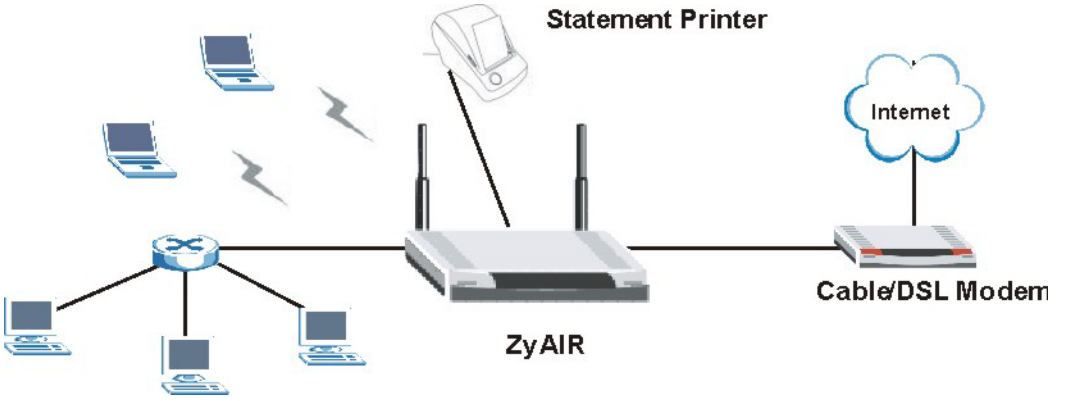


Figure 1-2 Application: Internet Access in Public Areas

Chapter 2
The Web Configurator

This chapter introduces how to access the web configurator to perform general system configuration.

2.1 Introducing the Web Configurator

The web configurator is best viewed with Internet Explorer (version 4.0 or above) or Netscape Navigator (version 6.0 or above). Your browser must have JavaScript support enabled.

2.2 Accessing the Web Configurator

Follow the steps below to access the web configurator.

The ZyAIR allows only one web configurator session at any one time.

Step 1. Make sure your ZyAIR is properly connected (refer to instructions in the *Quick Installation Guide* on hardware installtion and connections).

Step 2. Launch your web browser and type the WAN or LAN IP address of the ZyAIR as the web address (it is recommended that you connect your computer to the LAN and use the LAN IP address for initial configuration). **192.168.1.1** is the default IP address for the LAN port.
If you are using a different port number (between 8000 and 8099) for the web server, you must also append the port number to the LAN IP address seperated with a colon ":", for example, http://192.168.1.1:8080.

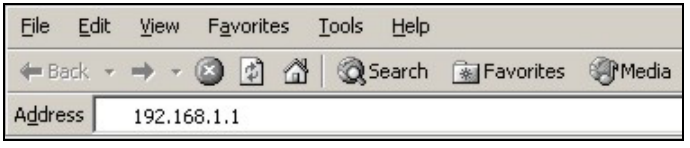


Figure 2-1 Entering ZyAIR IP Address in Internet Explorer

Step 3. A login screen displays. Type "admin" (default) as the user name and "1234" (default) as the password and click **Login**.

The user name and password are case sensitive.

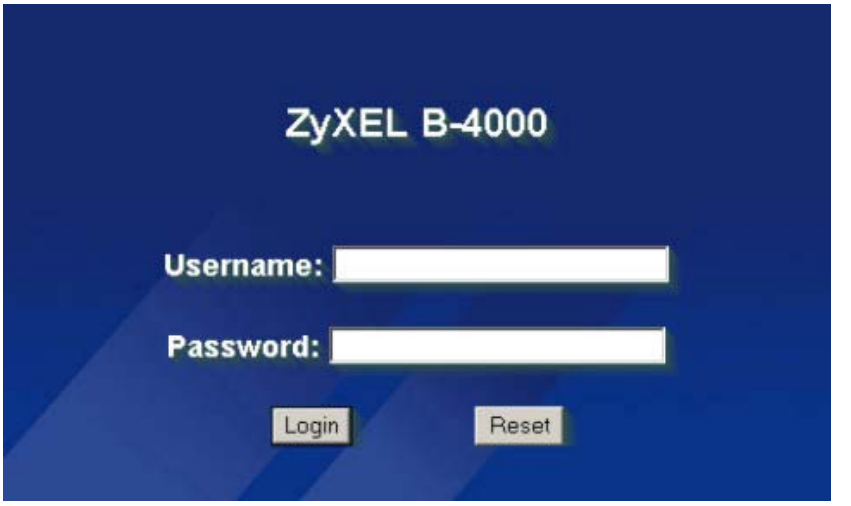


Figure 2-2 Web Configurator: Login

Step 4. You should see the first screen of the Wizard Setup. Refer to the *Quick Installation Guide* for more information on configuring the Wizard Setup screens.

The ZyAIR automatically logs you out if there is no activity for longer than five minutes after you log in. If this happens, simply log back in again. You can change the time period in the ADVANCED SERVER **screen's** Administrator Inactivity Timer **field.**

2.3 Wizard Setup Screens

The Wizard Setup screens display when you first access the ZyAIR. Refer to the *Quick Installation Guide* for information on how to configure the Wizard Setup screens.

2.4 Navigating the Web Configurator

After you finish the Wizard Setup screens, you first see the **Quick View** screen after login.

Click the HELP icon (located in the top right corner of most screens) to view online help.

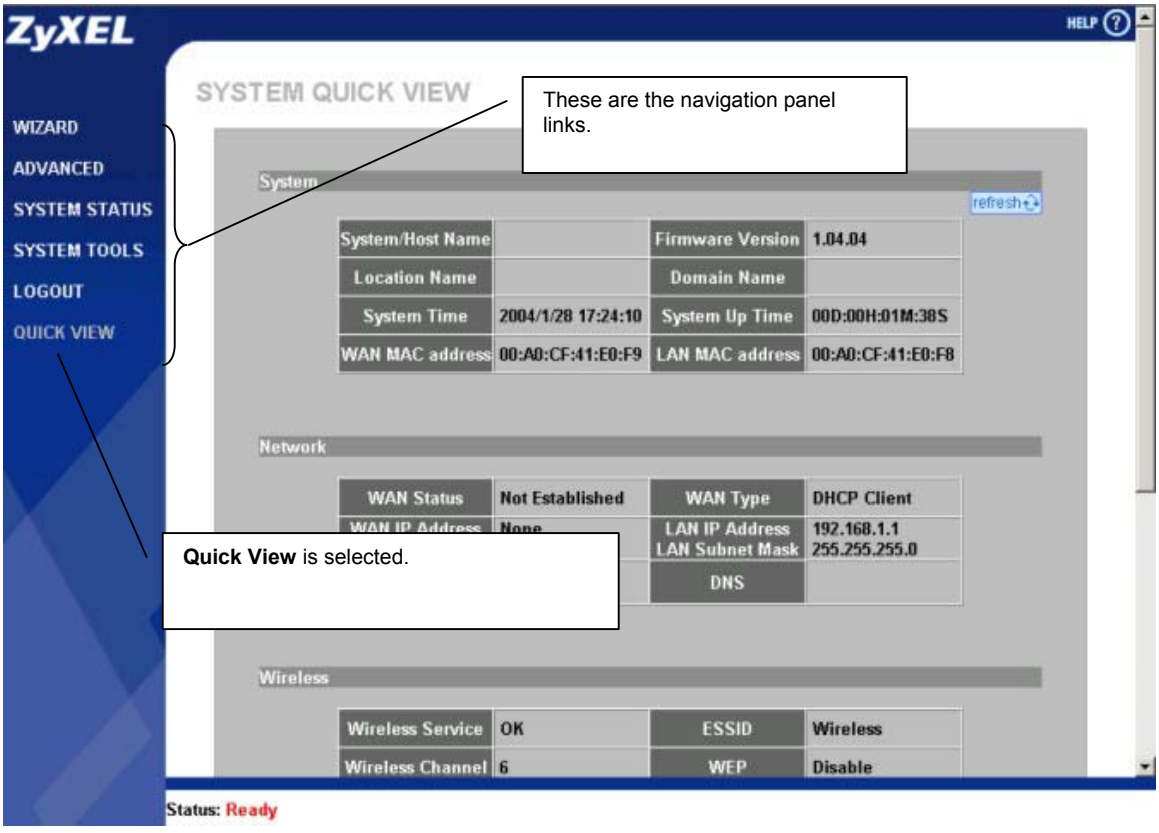


Figure 2-3 Web Configurator Navigation

Click a navigation panel link to open a submenu of links to individual screens. For example, click **WIZARD** to display the following submenu.

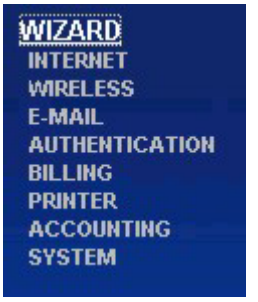


Figure 4 WIZARD Submenu

2.5 Screens Overview

The following table lists the various web configurator screens.

Table 2-1 Web Configurator Screens Overview

WIZARD	ADVANCED	SYSTEM STATUS	SYSTEM TOOLS
INTERNET	SYSTEM	SYSTEM	CONFIGURATION
WIRELESS	WAN/LAN	ACCOUNT LIST	FIRMWARE
E-MAIL	SERVER	ACCOUNT LOG	Manual Firmware Upgrade
AUTHENTICATION	AUTHENTICATION	CURRENT USER	Schedule Firmware Upgrade
BILLING	BILLING	DHCP CLIENT	SYSTEM ACCOUNT
PRINTER	ACCOUNTING	SESSION LIST	SSL CERTIFICATE
ACCOUNTING	CREDIT CARD	LAN DEVICES	PING COMMAND
SYSTEM	KEYPAD		RESTART

Table 2-1 Web Configurator Screens Overview			
WIZARD	**ADVANCED**	**SYSTEM STATUS**	**SYSTEM TOOLS**
	CUSTOMIZATION Login Page Logo Information Window Account Printout Credit Card PASS THROUGH FILTERING SHARE PORTAL PAGE ADVERTISEMENT WALLED GARDEN DDNS LAN DEVICES SYSLOG Syslog Log Settings WIRELESS WEP Key Setting		

Figure 5 Quick View

The following table describes the labels in this screen.

Table 2-2 Quick View

LABEL	DESCRIPTION
System	
Refresh	Click **Refresh** to update this screen.

Table 2-2 Quick View

LABEL	DESCRIPTION
System/Host Name	This field displays the description name of the ZyAIR for identification purposes.
Firmware Version	This field displays the version of the firmware on the ZyAIR.
Location Name	This field displays the device's geographical location.
Domain Name	This field displays the domain name of the ZyAIR.
System Time	This field displays the ZyAIR's current time.
System Up Time	This field displays the how long the ZyAIR has been operating since it was last started.
WAN MAC Address	This field displays the MAC address of the ZyAIR on the WAN.
LAN MAC Address	This field displays the MAC address of the ZyAIR on the LAN.
Network	
WAN Status	This field displays the status of the ZyAIR's connection to the Internet (**Established** or **Not Established**).
WAN Type	This field displays the DHCP mode of the WAN port. It displays **DHCP Client**, **Static IP Setting**, **PPPoE**, or **PPTP**.
WAN IP Address WAN Subnet Mask	This field displays the IP address and the subnet mask of the WAN port on the ZyAIR.
LAN IP Address LAN Subnet Mask	This field displays the IP address and the subnet mask of the LAN port on the ZyAIR.
Default Gateway	This field displays the IP address of the default gateway of the WAN port on the ZyAIR.
DNS	This field displays the IP address of the DNS server that the ZyAIR is using.
Wireless	
Wireless Service	This field displays the status of the ZyAIR's wireless LAN.
ESSID	This field displays the ZyAIR's Extended Service Set IDentity.

Table 2-2 Quick View

LABEL	DESCRIPTION
Wireless Channel	This field displays the channel that the ZyAIR is using.
WEP	This field displays whether the ZyAIR is using WEP data encryption.
Traffic	
WAN	This field displays traffic statistics for the ZyAIR's WAN connection.
LAN	This field displays traffic statistics for the ZyAIR's LAN connection.
Wireless	This field displays traffic statistics for the ZyAIR's wireless LAN connection.

2.6 Login Accounts

There are four system accounts that you can use to log in to the ZyAIR: administrator, account manager, supervisor and super subscriber.

The administrator account allows you full access to all system configurations. The default administrator user name is "admin" and the default password is "1234".

The account manager account is used for proprietary subscriber account management only. No system configuration is allowed. This account is useful for front desk personnel (such as in a hotel) for setting up subscriber accounts without tampering with the system configuration. The account manager default user name and password are "account".

With the supervisor account, you can only view the system status and change the supervisor account password. This account is useful for allowing a manager to view the device's status and lists of accounts and logged in subscribers without changing the system configuration. The default supervisor account user name and password are "supervisor".

Use the super subscriber account to test the Internet connection between the ZyAIR and the ISP. The ZyAIR does not impose time limitations or charges on this account. Thus, anyone who logs in with this account is able to gain Internet access for free. The default super subscriber user name and password are "super".

You can only log in using the super subscriber account in the subscriber login screen.

2.6.1 Changing Login Account Usernames and Passwords

It is recommended you change the account passwords.

Click **SYSTEM TOOLS** and **SYSTEM ACCOUNT**.

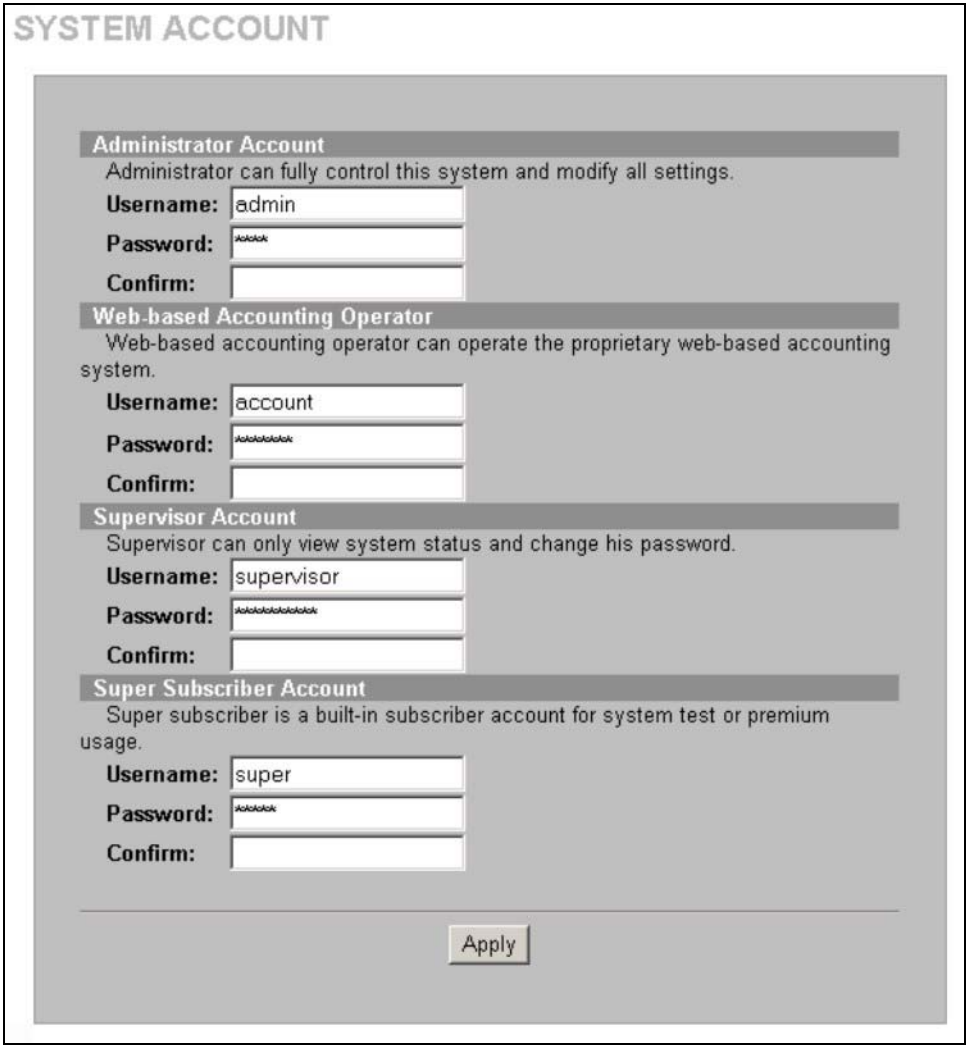


Figure 2-6 SYSTEM TOOLS: SYSTEM ACCOUNT

The account user names and passwords are case sensitive.

Table 2-3 SYSTEM TOOLS: SYSTEM ACCOUNT

LABEL	DESCRIPTION
Administrator Account	
Username	Enter the user name for the administrative account. The default is **admin**.
Password	Enter a new administrative account password.
Confirm	Enter the new administrator password again for confirmation.
Web-based Accounting Manager	
Username	Enter the user name for the account manager account. The default is **account**.
Password	Enter a new account manager password.
Confirm	Enter the new account manager password again for confirmation.
Supervisor Account	
Username	Enter the user name for the supervisor account. The default is **supervisor**.
Password	Enter a new supervisor password.
Confirm	Enter the new supervisor password again for confirmation.
Super Subscriber Account **You can only log in using the super subscriber account in the subscriber login screen.**	
Username	Enter the user name for the super subscriber account. The default is **super**.
Password	Enter a new super subscriber account password.
Confirm	Enter the new super subscriber account password again for confirmation.
Apply	Click **Apply** to save the changes back to the ZyAIR.

2.7 Methods of Restoring Factory-Defaults

There are two methods you can use to erase the current configuration and restore factory defaults.

2.7.1 Using the Reset Button to Restore Factory-Defaults

The reset button is located on the left side panel. Use a pointed object to press this button in once to reset the ZyAIR back to the factory defaults.

All of your custom configuration including the local subscriber database will be erased.

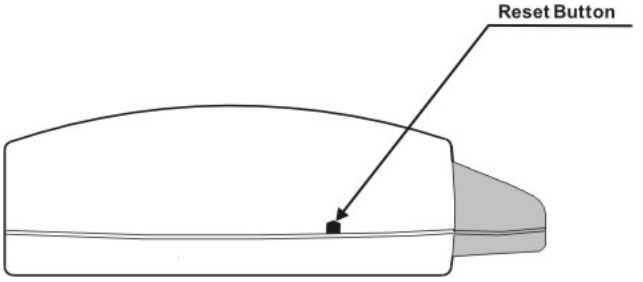


Figure 2-7 Side Panel

2.7.2 Using the Web Configurator to Restore Factory-Defaults

To reset the ZyAIR back to the factory defaults, click **SYSTEM TOOLS** and **DEFAULT SETTINGS** to display the screen as shown next.

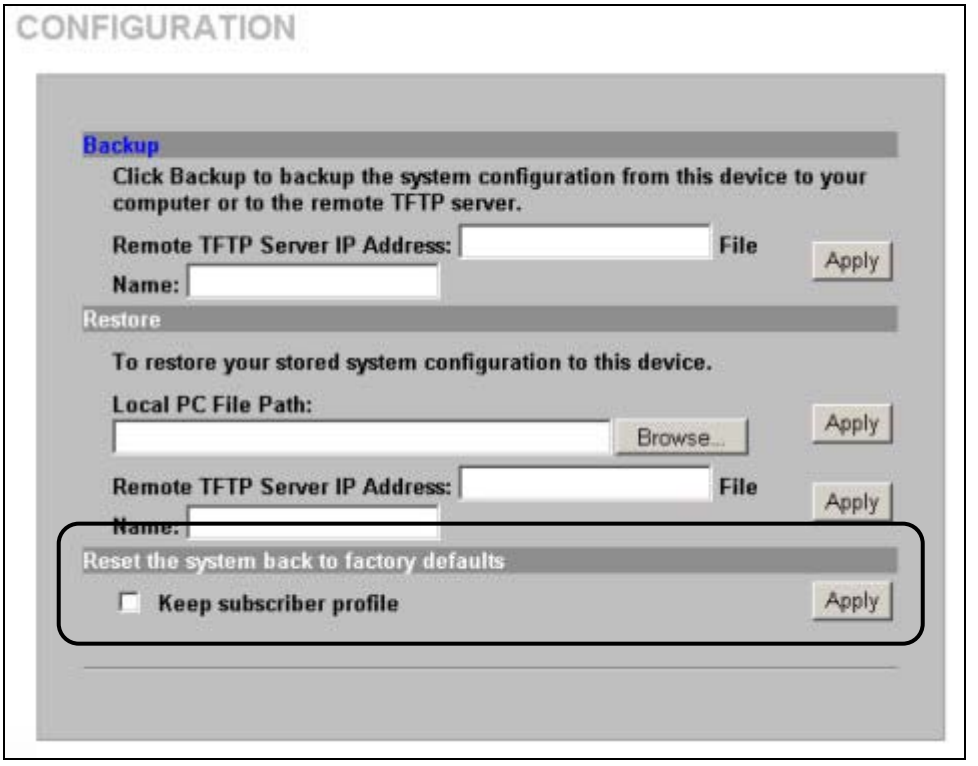


Figure 2-8 Reset to Default Settings

The following table describes the labels in this screen.

Table 2-4 Reset to Default Settings

LABEL	DESCRIPTION
Keep subscriber profile	Select this option to reset the system configuration back to the factory default but retain subscriber account information. All other custom configuration is erased.
Reset the system back to factory defaults	Click **Apply** to reset system configuration back to the factory defaults.

2.8 Restarting the ZyAIR

You *must* restart the ZyAIR every time you change the system IP address or upload a firmware or configuration file.

Click **SYSTEM TOOLS**, **RESTART** and then **Apply**.

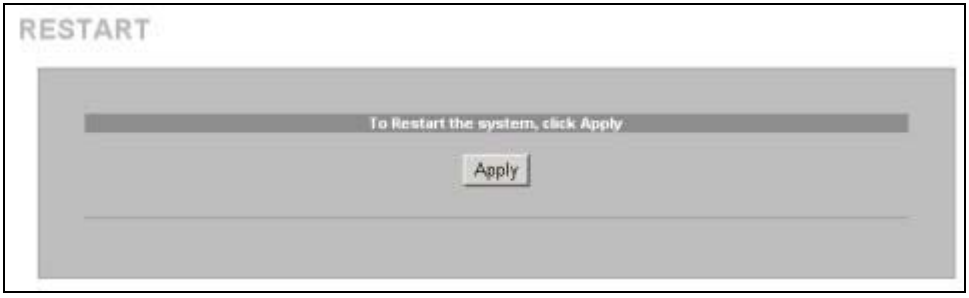


Figure 2-9 Restart

When the ZyAIR restarts, all connections will be terminated. Anyone using a system account will need to log in again. The subscribers may also need to log in again.

2.9 Logging Out of the Web Configurator

Click **LOGOUT** to exit from the web configurator.

Figure 2-10 Logging Out

Chapter 3
General System Setup

*This chapter describes how to configure the **SYSTEM** advanced setup screens.*

3.1 General System Settings

Click **ADVANCED** and then **SYSTEM** to open this screen.

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

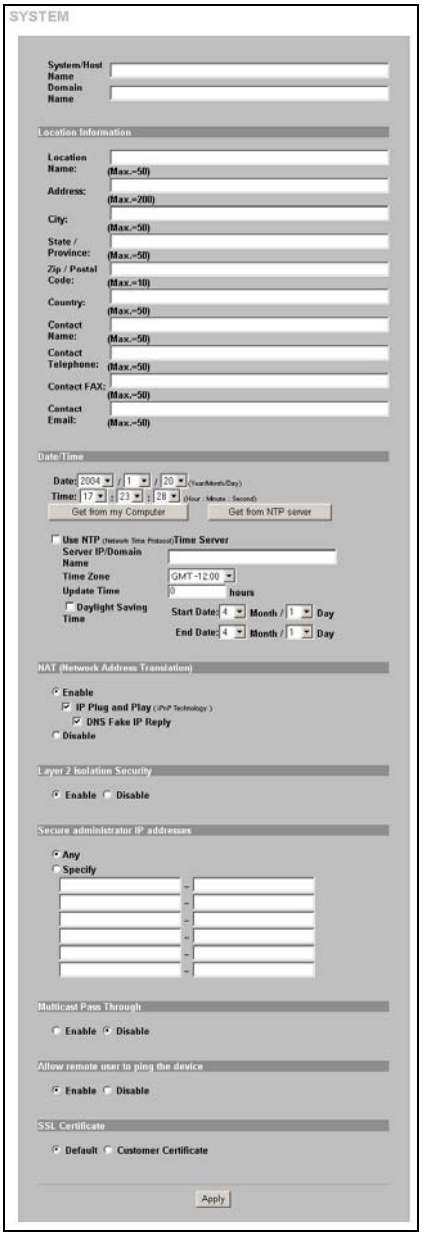


Figure 3-1 SYSTEM

The following table describes the labels in this screen.

Table 3-1 SYSTEM

LABEL	DESCRIPTION
System Name	Enter a descriptive name (up to 40 characters) for identification purposes.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ZyAIR may obtain a domain name from a DHCP server. The domain name entered by you is given priority over the DHCP server assigned domain name.
Location Information	
Location Name	Enter the device's geographical location.
Address	Enter the street address of the device's location.
City	Enter the city of the device's location.
State/Province	Enter the state or province of the device's location.
ZIP/ Postal Code	Enter the zip code or postal code for the device's location.
Country	Enter the country of the device's location.
Contact Name	Enter the name of the person responsible for this device.
Contact Telephone	Enter the telephone number of the person responsible for this device.
Contact FAX	Enter the fax number of the person responsible for this device.
Contact Email	Enter the e-mail address of the person responsible for this device.
Date/Time	Set the system date and time by selecting the appropriate choices from the drop-down list boxes.
Get from my Computer	Click this button to set the time and date on the ZyAIR to be the same as the management computer.
Get from NTP server	Click this button to set the time and date on the ZyAIR to be the same as the management computer.
Use NTP (Network Time Protocol) Time Server	Select this check box to set the ZyAIR to get time and date information from an NTP (Network Time Protocol) time server.
Server IP/Domain Name	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.

Table 3-1 SYSTEM

LABEL	DESCRIPTION
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Update Time	Enter a number to determine how often the ZyAIR uses the NTP server to update the time and date.
Daylight Saving	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	Select the month and day that your daylight-savings time starts on if you selected **Daylight Saving**.
End Date	Select the month and day that your daylight-savings time ends on if you selected **Daylight Saving**.
NAT (Network Address Translation)	Enable NAT to have the ZyAIR translate Internet protocol addresses used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). See the *LAN Devices* chapter for more on NAT.
IP Plug and Play (IPnP Technology)	Activate IP Plug and Play (iPnP) to allow computers to connect to the ZyAIR or access the Internet through the ZyAIR without changing their network configuration. This allows computers with static IP addresses that are not in the same subnet as the ZyAIR's LAN IP address to connect to the ZyAIR or access the Internet through the ZyAIR. When you disable iPnP, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyAIR's LAN IP address can connect to the ZyAIR or access the Internet through the ZyAIR.
DNS Fake IP Reply	Some subscribers' Internet browsers may be set to use an HTTP proxy with a private domain. Select this option to have the ZyAIR send a default IP address (169.254.1.1) in response to DNS queries. This way the subscribers' computers can send HTTP requests that the ZyAIR can redirect so the subscribers can login.
Layer 2 Isolation Security	If you activate NAT, select **Enable** in this field to prevent communication between subscribers. This is the default selection. Select **Disable**, to deactivate layer 2 security and allow communication between subscribers.

Table 3-1 SYSTEM

LABEL	DESCRIPTION
Secure administrator IP addresses	Select **Any** to use any computer to access the web configurator on the ZyAIR. Select **Specify** and then enter the IP address(es) or ranges of IP addresses of the computer(s) that are allowed to log in to configure the ZyAIR. The addresses can be on the LAN or the WAN.
Multicast Pass Through	Select **Enable** to allow multicast traffic to pass through the ZyAIR. This may affect your network performance. Select **Disable** to prevent any multicast traffic from passing through the ZyAIR. This is the default setting.
Allow remote user to ping the device	This feature affects the security of the ZyAIR's WAN port. Ping (Packet INternet Groper) is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. Select **Enable** to have the ZyAIR respond to incoming Ping requests from the WAN. This is less secure since someone on the Internet can see that the ZyAIR is there by pinging it. Select **Disable** to have the ZyAIR not respond to incoming Ping requests from the WAN. This is more secure since someone on the Internet cannot see that the ZyAIR is there by pinging it.
SSL Certificate	Secure Socket Layer (SSL) security allows you to create secure connections between the ZyAIR and the management or subscriber computer(s). Select **Default** to use the default system-generated SSL certificate. Select **Customer Certificate** to use a certificate obtained from a certificate authority. Refer to the *SSL (Secure Socket Layer) Security* chapter for more information.
Apply	Click **Apply** to save the changes.

Chapter 4
WAN, LAN and Server Setup

This chapter shows you how to configure LAN and WAN ports and server settings.

4.1 Factory Ethernet Defaults

The Ethernet parameters of the ZyAIR are preset to the following values:

- Dynamic WAN IP address.
- LAN IP address of 192.168.1.1 with subnet mask of 255.255.255.0
- DHCP server enabled on the LAN with a 253 client IP address pool starting from 192.168.1.2.

These parameters should work for the majority of installations. If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

4.2 LANs and WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand, is an outside connection to another network or the Internet.

4.3 IP Address Assignment

A static IP is a fixed IP that the ZyAIR obtains from a DHCP server on a network. A dynamic IP is not fixed; the DHCP server provides an IP address to the ZyAIR each time it connects to the network. When an Ethernet device is configured to obtain a dynamic IP address from a DHCP server, it is known as a DHCP client.

4.4 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (Ethernet device) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyAIR has built-in DHCP server capability, which means it can assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client when this feature is activated. The ZyAIR can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

4.4.1 IP Address and Subnet Mask

Like houses on a street that share a common street name, the 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.

The Internet Assigned Number Authority (IANA) reserved a block of addresses specifically for private use (refer to *Section 4.4.2*); 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.

The subnet mask specifies the network number portion of an IP address.

4.4.2 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, 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:

```
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 it can be assigned from 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.*

4.5 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. The second is to obtain the DNS server information automatically when a computer is set as a DHCP client.

4.6 PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the ZyAIR (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyAIR does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

4.6.1 PPP MTU

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network. The Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled.

4.6.2 TCP MSS

The maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece. For optimum communications, the

number of bytes in the data segment and the header must add up to less than the number of bytes in the maximum transmission unit (MTU).

4.7 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

4.8 Configuring the WAN and LAN Settings

To configure the WAN and LAN settings on the ZyAIR, click **ADVANCED** and **LAN/WAN** to display the screen as shown.

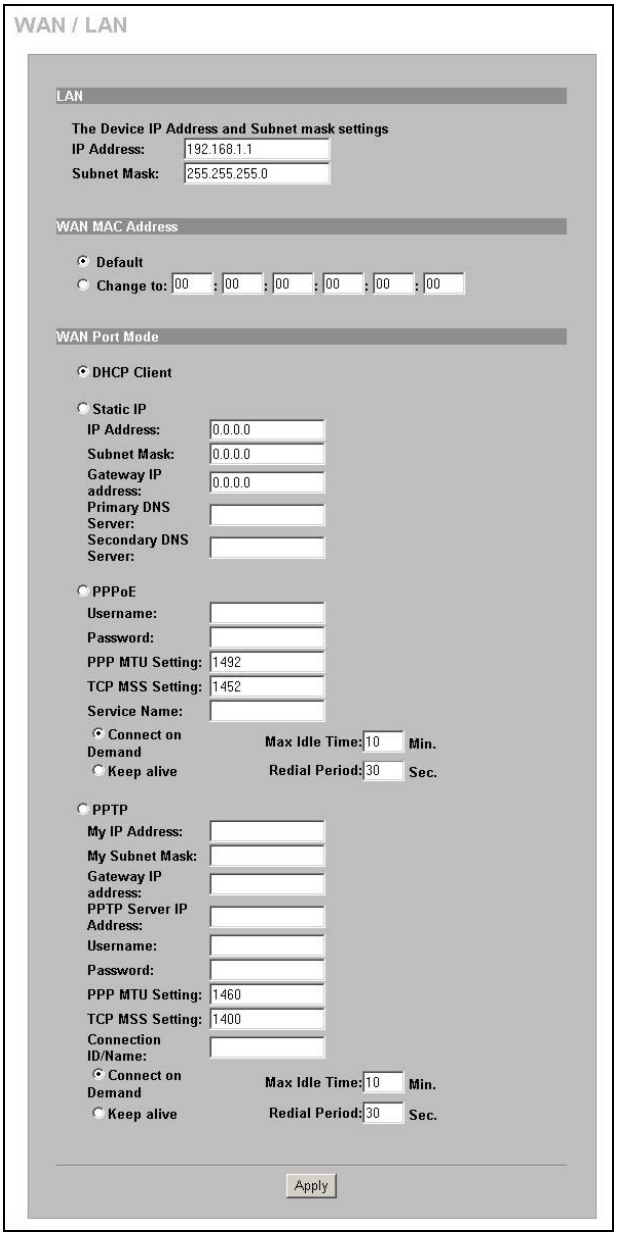


Figure 4-1 WAN/LAN

The following table describes the labels in this screen.

Table 4-1 WAN/LAN

LABEL	DESCRIPTION
LAN	
IP Address	Enter the LAN IP address of the ZyAIR in dotted decimal notation. The default is **192.168.1.1**.
Subnet Mask	Enter the LAN subnet mask in dotted decimal notation. The default is **255.255.255.0**.
WAN MAC Address	Select **Default** to use the factory assigned MAC address. If your ISP requires MAC address authentication, select **Change to** and enter the MAC address of a computer on the LAN in the fields provided.
WAN Port Mode	
DHCP Client	Select this option to set the ZyAIR to act as a DHCP client on the WAN. The ZyAIR obtains TCP/IP information (IP address, DNS server information, etc.) from a DHCP server. This is the default setting.
Static IP	Select this option to set the ZyAIR to use a static (or fixed) IP address.
IP Address	Enter the static IP address in dotted decimal notation.
Subnet Mask	Enter the subnet mask in dotted decimal notation.
Gateway IP address	Enter the IP address of the default gateway device.
Primary/Secondary DNS Server	Enter the IP addresses of the primary and/or secondary DNS servers.
PPPoE	Select this option to activate **PPPoE** support. Refer to *Section 4.6* for more information.
Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the MTU (Maximum Transfer Unit) size.
TCP MSS Setting	Enter the MSS (Maximum Segment Size) size.
Service Name	Enter the name of your PPPoE service.

Table 4-1 WAN/LAN

LABEL	DESCRIPTION
Connect on Demand	Select this option when you don't want the connection up all the time and specify an idle timeout in the **Max Idle Time** field. This is the default setting with an idle timeout of **10** minutes.
Keep Alive	Select this option when you want the Internet connection up all the time and specify a redial period in the **Redial Period** field. When disconnected, the ZyAIR will attempt to bring up the connection after the redial period.
PPTP	Select this option to activate **PPTP** support. Refer to *Section 4.7* for more information.
My IP Address	Enter the IP address assigned to you.
My Subnet Mask	Enter the subnet mask assigned to you.
Gateway IP address	Enter the IP address of the gateway device.
PPTP Server IP Address	Enter the IP address of your ISP's PPTP server.
Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the MTU (Maximum Transfer Unit) size.
TCP MSS Setting	Enter the MSS (Maximum Segment Size) size.
Connection ID/Name	Enter your identification name of the PPTP server assigned to you by the ISP.
Connect on Demand	Select this option when you don't want the connection up all the time and specify an idle timeout in the **Max Idle Time** field. This is the default setting with an idle timeout of **10** minutes.
Keep Alive	Select this option when you want the Internet connection up all the time and specify a redial period in the **Redial Period** field. When disconnected, the ZyAIR will attempt to bring up the connection after the redial period.
Apply	Click **Apply** to save the changes.

4.9 Server Configuration

Use the **SERVER** screen to set the embedded web server, the LAN DHCP server and specify the e-mail server for e-mail redirection on the ZyAIR.

Click the **ADVANCED SETUP** and **SERVER** to display the screen as shown next.

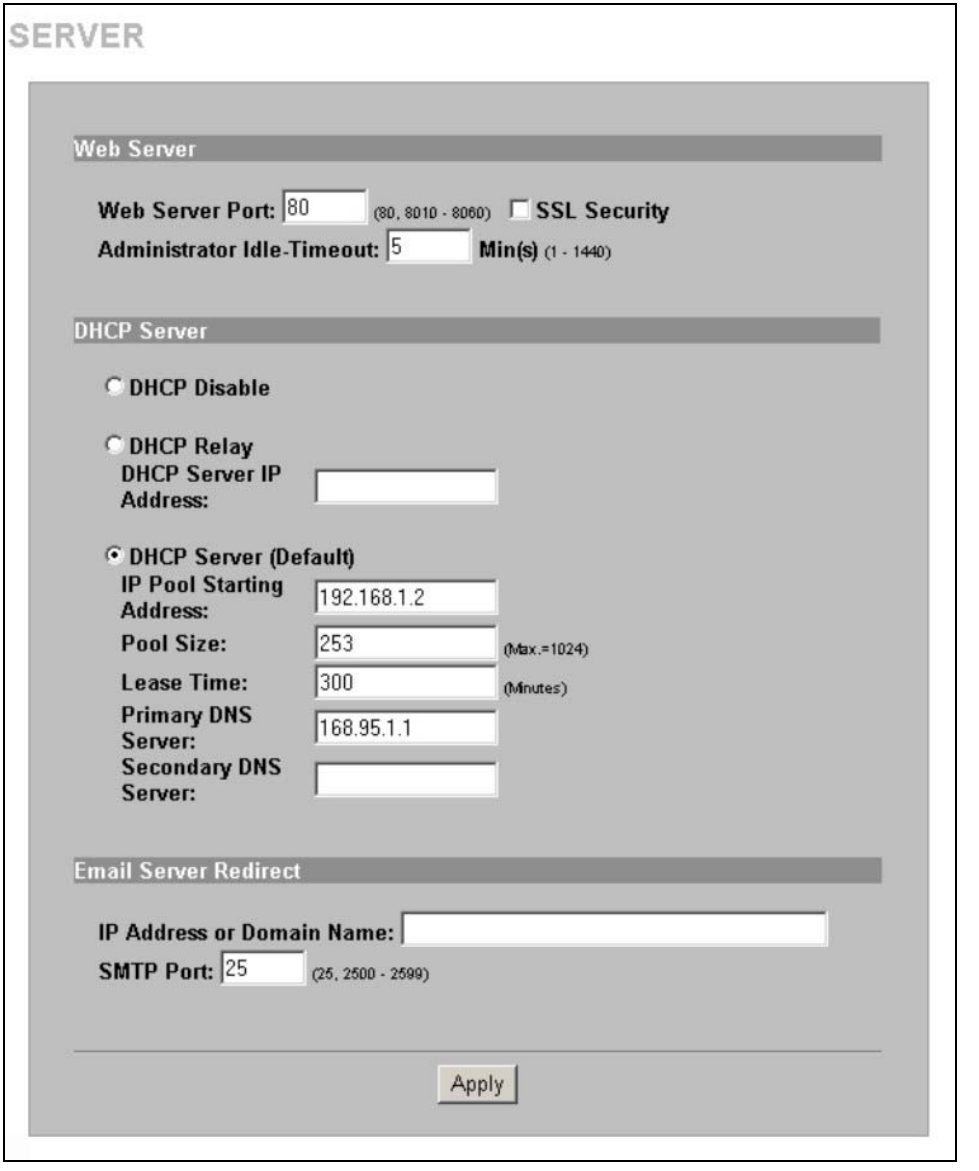


Figure 4-2 SERVER

The following table describes the fields in this screen.

Table 4-2 SERVER

LABEL	DESCRIPTION
Web Server	
Web Server Port	Specify the port number of the embedded web server on the ZyAIR for accessing the web configurator. The default port number is **80**. Changing the port number helps protect the ZyAIR's web configurator from hacker attacks. Enter a number between 8010 and 8060 to access the web configurator behind a NAT-enabled network. If you enter a number between 8000 and 8060, you need to append the port number to the **WAN** or **LAN** port IP address to access the web configurator. For example, if you enter "8010" as the web server port number, then you must enter "http://www.192.168.1.1:8010" where 192.168.1.1 is the WAN or LAN port IP address.
SSL Security	Secure Socket Layer (SSL) security allows you to create secure connections between the ZyAIR and the management computer(s). Refer to the *SSL (Secure Socket Layer) Security* chapter for more information. Select this check box to activate SSL security.
Administrator Idle-Timeout	Type how many minutes a management session 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).
DHCP Server Select the DHCP mode on the LAN.	
DHCP Disable	Select this option to disable DHCP server on the LAN.
DHCP Relay	Use this if you have a DHCP server (either a computer or another router) and you want that DHCP server to also assign network information (IP address, DNS information etc.) to the devices that connect to the ZyAIR. Select this option to set the ZyAIR to forward network configuration requests to a DHCP server. Then configure the **DHCP Server IP Address** field.
DHCP Server IP Address	If you select **DHCP Relay**, enter the IP address of a DHCP server (on the WAN).

Table 4-2 SERVER

LABEL	DESCRIPTION
DHCP Server (Default)	Select this option to set the ZyAIR to assign network information (IP address, DNS information etc.) to Ethernet device(s) connected to the **LAN** port(s). This is the default setting.
IP Pool Starting Address	Enter the first of the continuous addresses in the IP address pool. The default is **192.168.1.2**.
DHCP Pool Size	This field specifies the size or count of the IP address pool. Enter a number not greater than 1024. The default is **253**.
Lease Time	Specify the time (in minutes between 1 and 71582788) a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
Primary/Secondary DNS Server	Enter the IP address of the DNS server(s) in the **Primary DNS IP Address** and/or **Secondary DNS IP Address** fields. **You *must* specify a DNS server.**
E-mail Server Redirect	
IP Address or Domain Name	Specify the IP address or the domain name of the e-mail server to which the ZyAIR forwards e-mail.
SMTP Port	Enter the port number (25, or between 2500 and 2599) for the mail server. The default is **25**.
Apply	Click **Apply** to save the settings.

Part II:

Subscriber Account Management

This part covers the **ADVANCED AUTHENTICATION**, **BILLING**, **ACCOUNTING** and **CREDIT CARD** screens.

Chapter 5 Authentication

This chapter shows you how to set up subscriber authentication on the ZyAIR.

5.1 About the Built-in Authentication

You can use the built-in subscriber database to manage the subscribers. The ZyAIR also provides a built-in billing mechanism to set up accounting information without using accounting software or an accounting server (such as RADIUS).

5.2 Authentication Settings

Click **ADVANCED** and **AUTHENTICATION** to display the screen as shown next.

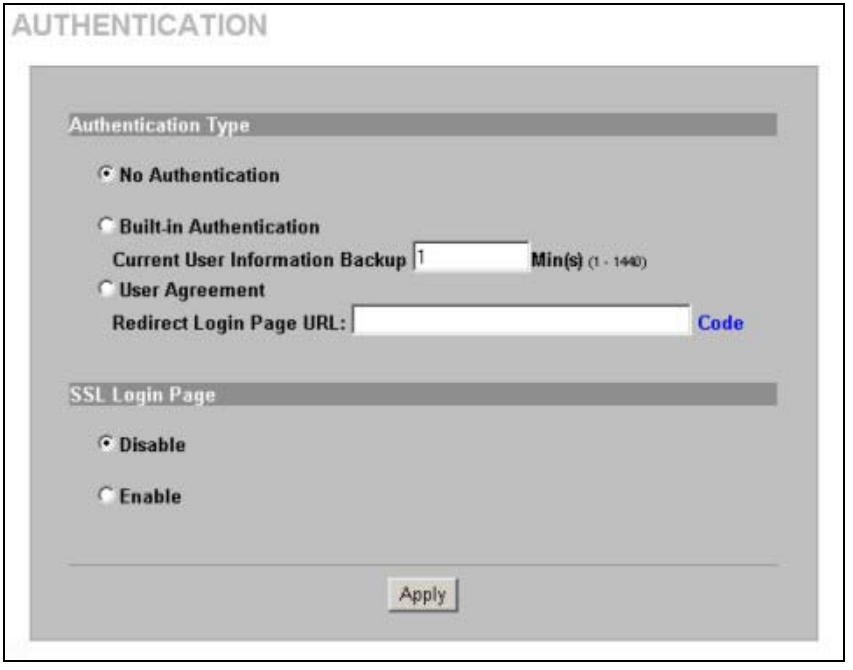


Figure 5-1 AUTHENTICATION

The following table describes the labels in this screen.

Table 5-1 AUTHENTICATION

LABEL	DESCRIPTION
No Authentication	Select this option to disable subscriber authentication. Subscribers can access the Internet without entering user names and passwords. This is the default setting.
Built-in Authentication	Select this option to authenticate the subscribers using the local subscriber database. **When you select this option, you *must* also configure the** Accounting **screen.**
Current User Information Backup	The system provides automatic backup of account information and status. Use this field to set the number of minutes between backups. The default value is 1 minute. The valid range is 1 to 1440. If you create a subscriber account and the ZyAIR restarts before backing up the account information, the subscriber account will not be saved. You will need to create a new account for the subscriber.
User Agreement	Select **User Agreement** to redirect a subscriber to an Internet service usage agreement page before accessing the Internet.
Redirect Login Page URL	Specify the URL of the user agreement page in the field provided. Click **Code** to display the HTML source code of a default sample page. The user agreement page must include the HTML source code in the default sample page in order for user agreement page to send the subscribers' agreement or disagreement to the ZyAIR.
SSL Login Page Security	Select **Enable** to activate SSL security upon accessing the subscriber login screen so that the subscribers' user names and passwords are encrypted before being transmitted to the ZyAIR. This applies when you select **Built-in Authentication** or **User Agreement**. Select **Disable** to de-activate SSL security for the subscriber login screen. Refer to the *SSL (Secure Socket Layer) Security* chapter for more information.
Apply	Click **Apply** to save the changes.

Chapter 6
Billing

This chapter shows you how to set up subscriber billing on the ZyAIR.

6.1 About the Built-in Billing

You can use the built-in billing function to setup billing profiles. A billing profile describes how to charge subscribers.

6.1.1 Accumulation Accounting Method

The accumulation accounting method allows multiple re-logins until the allocated time period or until the subscriber account is expired. The ZyAIR accounts for the time the subscriber logs in for Internet access.

6.1.2 Time-to-finish Accounting Method

The time-to-finish accounting method is good for one-time logins. Once a subscriber logs in, the ZyAIR stores the MAC address of the subscriber's computer for the duration of the time allocated. Thus the subscriber does not have to enter the user name and password again for re-login within the allocated time.

Once activated, the subscriber account is valid until the allocated time is reached even if the subscriber disconnects Internet access for a certain period within the allocated time. For example, Joe purchases a one-hour time-to-finish account. He starts using the Internet for the first 20 minutes and then disconnects his Internet access to go to a 20-minute meeting. After the meeting, he only has 20 minutes left on his account.

6.2 Billing Settings

Click **ADVANCED** and **BILLING** to display the screen as shown next.

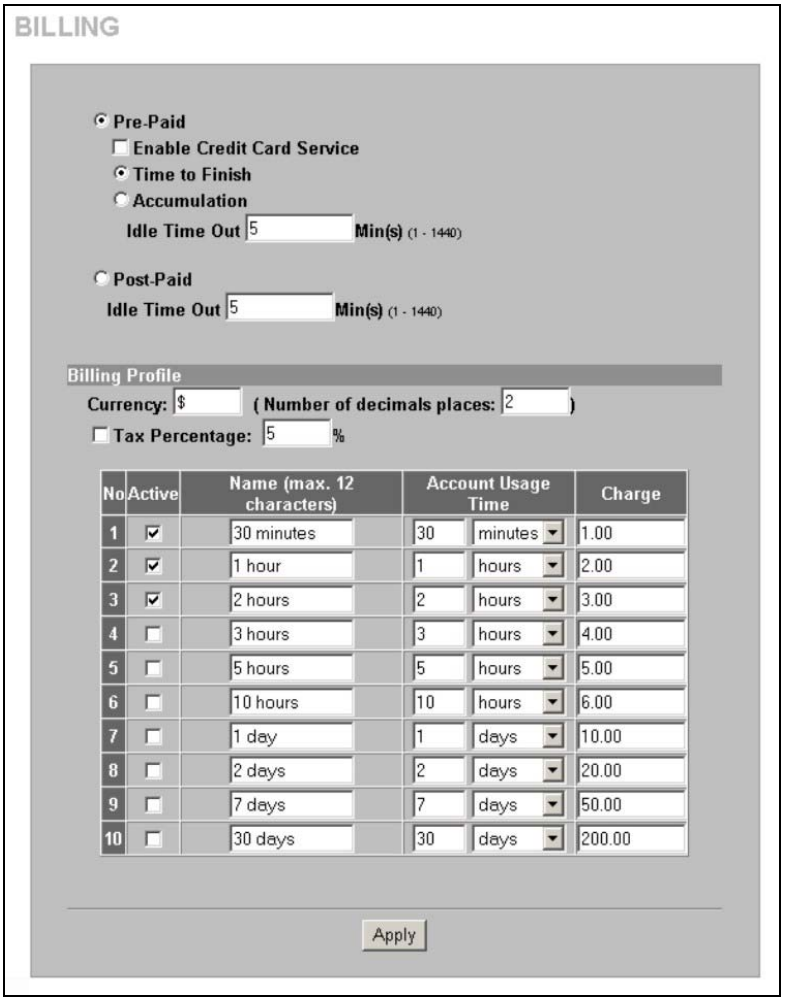


Figure 6-1 BILLING

The following table describes the labels in this screen.

If you change the billing mode, the system erases all accounts and disconnects all on-line subscribers.

Table 6-1 BILLING

LABEL	DESCRIPTION
Pre-Paid	Enable this option to allow the subscribers to access the Internet for a pre-defined time period.
Enable Credit Card Service	Enable the credit card service to authorize, process, and manage credit transactions directly through the Internet. Before you enable credit card service, make sure that your credit service is configured to work and the currency is American dollars. You must convert all prices on your billing page into American dollars (U.S. dollars). See the section on credit card for details.
Time to Finish	Select this option to allow each subscriber a one-time login. Once the subscriber logs in, the system starts counting down the pre-defined usage even if the subscriber stops the Internet access before the time period is finished. If a subscriber disconnects and reconnects before the allocated time expires, the subscriber does not have to enter the user name and password to access the Internet again.
Accumulation	Select this option to allow each subscriber multiple re-login until the time allocated is used up.
Idle Time Out	The ZyAIR automatically disconnects a computer from the network after a period of inactivity. The subscriber may need to enter the username and password again before access to the network is allowed. Specify the idle timeout between 1 and 1440 minutes. The default is **5** minutes.
Post-Paid	A subscriber can access the Internet without a pre-defined usage time. The printout only shows the username and password. The hot spot operator can also use the optional keypad to terminate an account. **Only the three-button printer with an optional keypad supports the post-paid function.**
Idle Time Out	The ZyAIR automatically disconnects a computer from the network after a period of inactivity. The subscriber may need to enter the username and password again before access to the network is allowed. Specify the idle timeout between 1 and 1440 minutes. The default is **5** minutes.
Currency	Enter the appropriate currency unit or currency symbol.
Number of decimals places	Define the number of decimal places (up to 3) to be used for billing.

Table 6-1 BILLING

LABEL	DESCRIPTION
Tax Percentage	Select this check box to charge sales tax for the account. Enter the tax rate (a 5% sales tax is entered as 5).
No.	The index numbers of the billing profiles.
Active	Select the check box, to activate the billing profile or clear the check box to deactivate the billing profile.
Name	Enter a name (up to 12 characters) for the billing profile.
Account Usage Time	Use these fields to set the duration of the billing period. When this period expires, the subscriber's access will be stopped. Select a time period (**minutes**, **hours**, or **days**) and enter the time unit in the field provided to define each "profile's" maximum Internet access time.
Charge	Define each profile's price, up to 999999, per time unit (configured in the **Account Usage Time** field).
Apply	Click **Apply** to save the changes.

Chapter 7
Accounting

This chapter shows you how to set up and manage subscriber accounts.

7.1 About Subscriber Accounts

Once the time allocated to a dynamic account is used up or a dynamic account remains un-used after the expiration time, the account is deleted from the account list. Accounts are automatically generated either by pressing the connected exclusive printer's button or using the web configurator (the **Account Generator Panel** screen).

7.2 Discount Price Plan

You can configure a custom discount pricing plan. This is useful for providing reduced rates for purchases of longer periods of time. You can charge higher rates per unit at lower levels (fewer units purchased) and lower rates per unit at higher levels (more units purchased).

The discount price plan only works when the hot spot operator does the billing through the statement printer or the web-based account generator panel. The discount price plan does not apply to subscribers purchasing access time online with a credit card.

7.2.1 Charge By Levels

The discount price plan gives you the option to charge by levels. This allows you to charge the rate at each successive level from the first level (most expensive per unit) to the highest level (least expensive per unit) that the total purchase reaches.

Otherwise you can disable the charge by level function and charge all of the time units only at the highest (least expensive) level that the total purchase reaches.

See *section 7.3.1* for an example of the charge by levels accounting function.

7.3 Accounting Settings

Click **ADVANCED** and **ACCOUNTING** to display the screen as shown next.

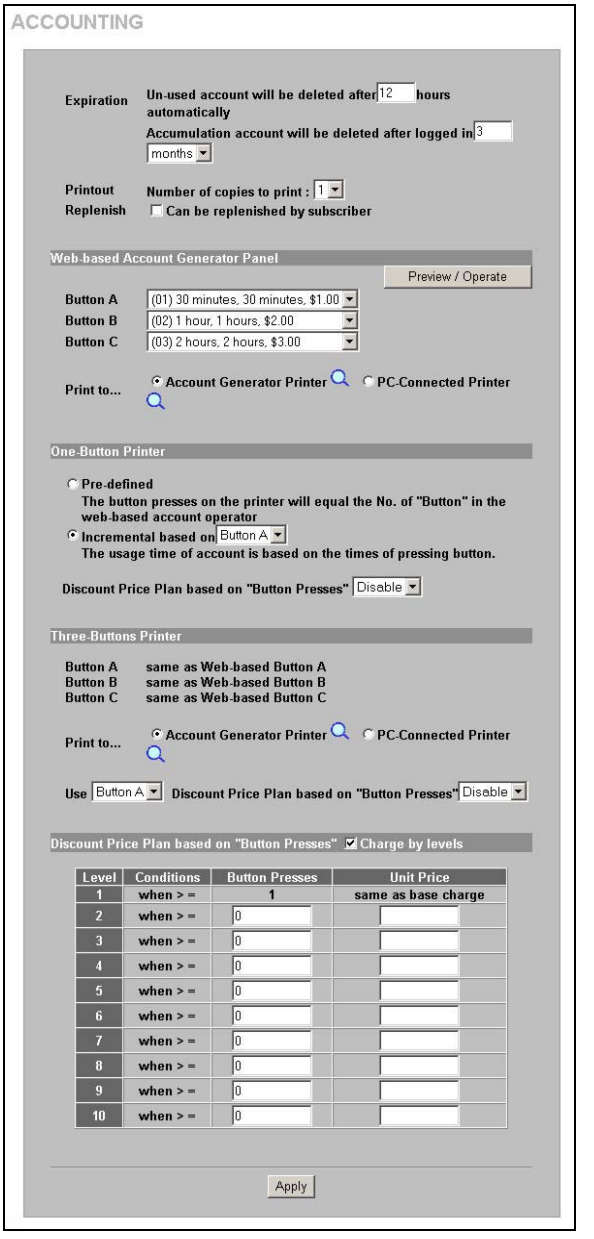


Figure 7-1 ACCOUNTING

The following table describes the labels in this screen.

Table 7-1 ACCOUNTING

LABEL	DESCRIPTION
Expiration	
Un-used account will be deleted after ~hours automatically	Specify the number of hours (1 to 168) to wait before the ZyAIR deletes an account that has not been used (default 12). This is for use with time to finish accounting.
Accumulation account will be deleted after logged in	Enter the number and select a time unit from the drop-down list box to specify how long to wait before the ZyAIR deletes an idle account. This is for use with accumulation accounting.
Printout	
Number of copies to print	Select how many copies of subscriber statements you want to print (1 is the default).
Replenish	
Can be replenished by subscriber	Select the check box to allow subscribers to purchase additional time units for their accounts before the accounts expire.
Web-based Account Generator Panel	
Preview/Operate	Click **Preview/Operate** to open the **Account Generator Panel** (see *Figure 7-3*).
Button A~C	Each button represents a billing profile that defines maximum Internet access time and charge per time unit. The buttons correspond to the buttons displayed in the **Account Generator Panel**. Select a billing profile from the list box for each button.
Print to…	Select **Account Generator Printer** if you want to print the account information using a statement printer connected to the **CONSOLE** port on the ZYAIR. Select **PC-Connected Printer** if you want to print the account information using a printer connected to a network computer. Click the  icon to display a print preview.

Table 7-1 ACCOUNTING

LABEL	DESCRIPTION
One-Button Printer	
Use this section with the one-button exclusive printer.	
Pre-defined	Pressing the button on the printer will equal the buttons in the web-based account generator panel. Press the printer button once for button A, twice for button B and thrice for button C. Press the printer button four times and the printer cancels the action.
Incremental based on Button	The usage time of the subscriber account is based on how many times you press the printer's button. Use the drop-down list box to select the button to use for this function. If you set this to **Button A**, pressing the printer's button A once equals Button A above and pressing it three times equals Button A x 3.
Discount Price Plan based on "Button Presses"	You can define a discount plan below. Use this field to enable or disable the use of the discount price plan.
Three-Buttons Printer	
Use this section with the three-button exclusive printer.	
Button A~C	These buttons correspond to the **Web-based Account Generator Panel** section's buttons A~C. Each button represents a billing profile that defines maximum Internet access time and charge per time unit.
Print to…	Select **Account Generator Printer** if you want to print the account information using a statement printer connected to the **ONE-CLICK PRINTER** port on the ZYAIR. Select **PC-Connected Printer** if you want to print the account information using a printer connected to a network computer. Click the  icon to display a print preview.
Use ~ Discount Price Plan based on "Button Presses"	Select a button from the drop-down list box to assign the base charge and select **Enable** to activate the discount price plan.
Discount Price Plan based on "Button Presses"	

Table 7-1 ACCOUNTING

LABEL	DESCRIPTION
Charge by levels	Disable the charge by level function to charge all of the subscriber's time units only at the highest level (least expensive) that their total number of button presses reaches. Enable the charge by levels function to charge the subscriber the rates at each successive level from the first level (least expensive) to the highest level (least expensive) that their total number of button presses reaches.
Level	These are the read-only level numbers of the discount charges.
Conditions	A discount level takes effect whenever the button selected in the **Three button Printer Setting** section is pressed more than or the same number of times as the number displayed in the **Button Presses** field.
Button Presses	Enter the number of times the button must be pressed to equal that discount level.
Unit Price	Enter each level's charge per time unit.
Apply	Click **Apply** to save your settings to the ZyAIR.

7.3.1 Charge By Levels Example

This is an example of how charge by levels accounting works. The discount price plan allows you to make the unit price lower as the subscriber purchases more (meaning a higher number of button pushes). The **Unit Price** for level 1 is always the same as the base charge ($2.00 for this example). The following screen has discount price level 2 set to $1.75 and level 3 set to $1.50. Taxes are not included in this example.

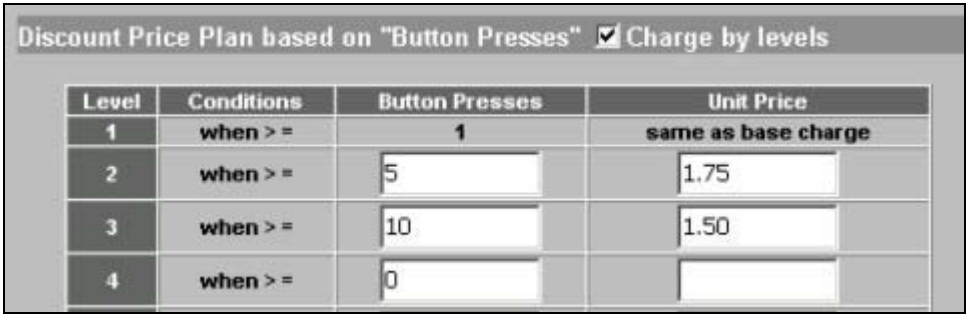


Figure 7-2 Charge By Levels Example

A subscriber purchases 11 units. Without charge by levels accounting, the total would be the number of button presses (11) multiplied by the unit price for the level that the number of button presses matches. In this case it would be 11x $1.50 for a total of $16.50 (excluding tax).

With charge by levels accounting, you charge the subscriber the rate at each successive level from the first level (most expensive per unit) to the highest level (least expensive per unit) that the purchase reaches. In this example, the ZyAIR would charge as follows:

Table 7-2 Charge By Levels Example

The base charge ($2.00) per unit for button presses 1-4.	($2.00 x 4= $8.00)
The level 2, unit price ($1.75) per unit for button presses 5-9.	($1.75 x 5= $8.75)
The level 3, unit price ($1.50) per unit for button presses 10-11.	($1.50 x 2= $3.00)
For a total of:	$19.75 (excluding tax)

7.4 Creating Accounts

There are two ways to create subscriber accounts: using the **Account Generator Panel** screen in the web configurator or using the exclusive printer.

7.4.1 Creating Accounts in the Web Configurator

To create subscriber accounts, click **Preview/Operate** in the **ACCOUNTING** screen to display the **Account Generator Panel** screen shown next.

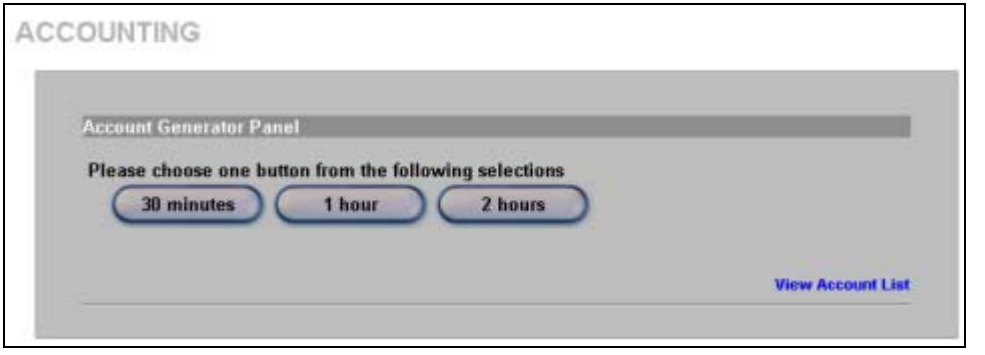


Figure 7-3 Account Generator Panel

The settings for the first button apply to the button on the exclusive printer.

Click a button to generate an account based on the settings you configure for the button in the **ACCOUNTING** screen. A window displays showing a printout preview of the account generated.

The following figure shows an example. Close this window when you are finished viewing it.

Figure 7-4 Web-based Account Generator Printout Preview Example

Figure 7-5 Web-based PC-connected Printout Preview Example

7.4.2 Using the Exclusive Printer to Create and Print Subscriber Statements

Follow the steps below to setup and create subscriber accounts and print subscriber statements using an external statement printer.

Step 1. Make sure that the printer's is connected to the appropriate power and the ZyAIR, and that there is printing paper in the statement printer. Refer to the printer's *User's Guide* for details.

Step 2. Press the button on the statement printer. The ZyAIR generates a dynamic account and the printer prints the subscriber's statement. Refer to *Figure 7-4* for a printout example.

The one-button statement printer's button corresponds to the first button in the Account Generator Panel **screen. Refer to *Figure 7-3*.**

Refer to section *7.3* to configure the printout page.

7.5 Viewing the Account List

Do one of the following to view the account list.

- From the **Account Generator Panel** screen (refer to *Figure 7-3*) and click **View Account List**.
- From the **SYSTEM STATUS** sub-menus, click **ACCOUNT LIST**.

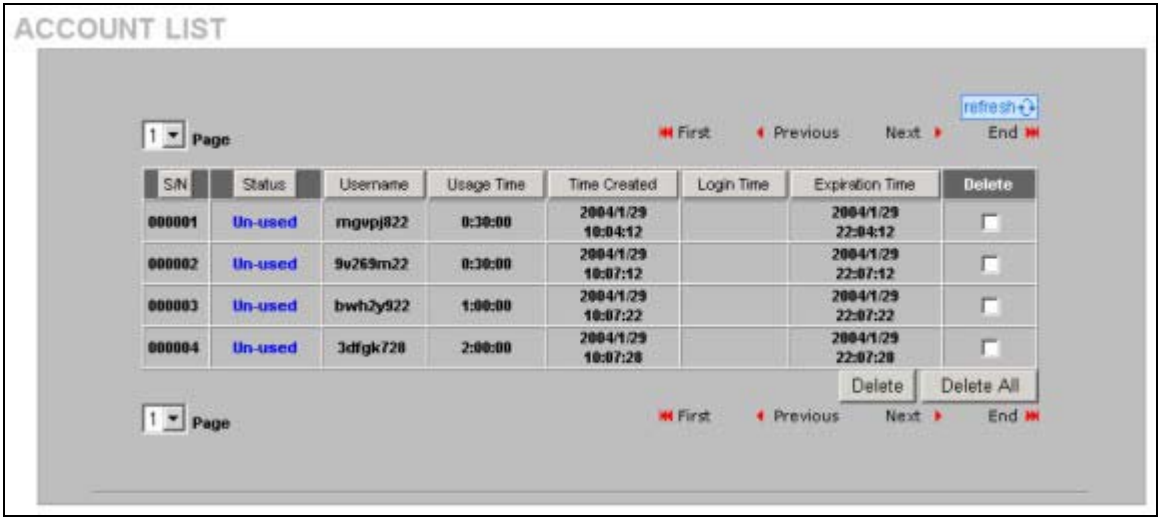


Figure 7-6 Account List

The following table describes the labels in this screen.

Table 7-3 Account List

LABEL	DESCRIPTION
Refresh	Click **Refresh** to update this screen.
S/N	This field displays the index number of an entry. The maximum number of subscriber account entries is 512.
Status	This field displays **IN-Used** when the account is currently in use. Otherwise it displays **UN-Used**.
Username	This field displays the account user name. Click the heading to sort the entries in ascending or descending order based on this column.
Usage Time	This field displays the amount of time the subscriber has purchased. Click the heading to sort the entries in ascending or descending order based on this column.

Table 7-3 Account List

LABEL	DESCRIPTION
Time Created	This field displays when the account was created (in yyyy/mm/dd hh/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Login Time	This field displays when the subscriber logged in to use the account (in yyyy/mm/dd hh/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Expiration Time	This field displays when the subscriber's account becomes invalid (in yyyy/mm/dd hh/mm/ss format). When the subscriber has already logged into the account, this field displays the time until which the subscriber can continue to use the account to access the Internet. When the subscriber has not yet logged into the account, this field displays the time that the account expires if the subscriber does not log into it. Click the heading to sort the entries in ascending or descending order based on this column.
Delete All	Click **Delete All** to remove all accounts.
Delete	Select the **Delete** checkbox(es) next to individual accounts and click **Delete** to remove the selected accounts.
Page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.

Refer to the *Subscriber Login* appendix for more information on logging in as a subscriber.

Chapter 8
Credit Card

This chapter shows you how to set the ZyAIR to handle credit card transactions.

8.1 About the Credit Card Screen

The ZyAIR allows you to use a credit card service to authorize, process, and manage credit transactions directly through the Internet. You must register with the Authorize.Net credit card service (www.authorizenet.com) before you can configure the ZyAIR to handle credit card transactions.

8.2 Credit Card Settings

Click **ADVANCED** and **CREDIT CARD** to display the screen as shown next.

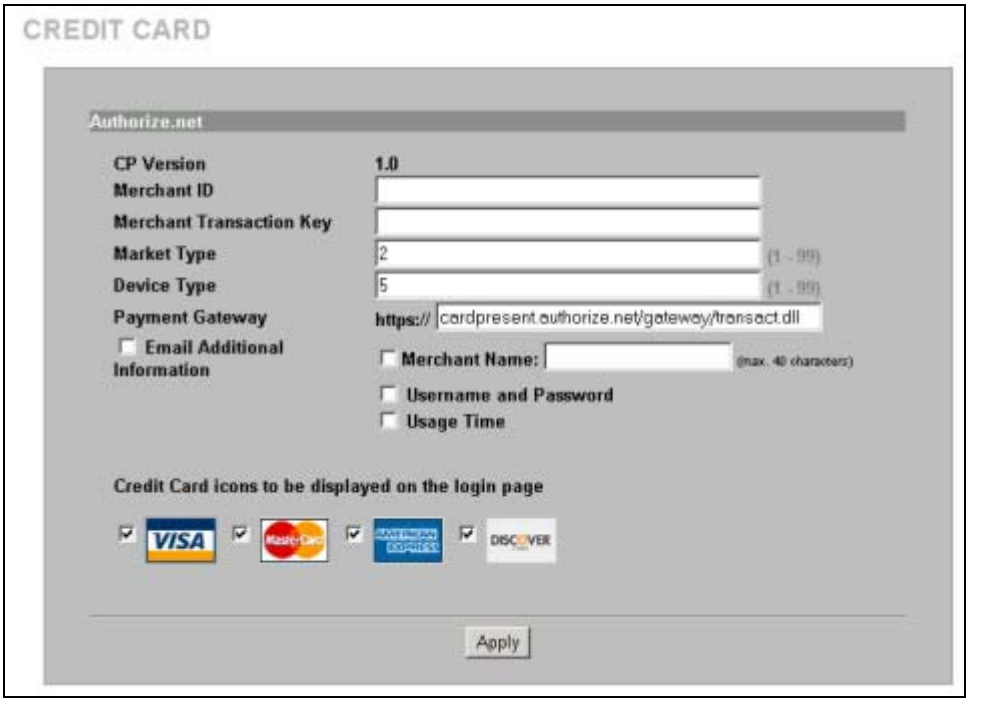


Figure 8-1 CREDIT CARD

The following table describes the labels in this screen.

Table 8-1 CREDIT CARD

LABEL	DESCRIPTION
Authorize.Net	
CP Version	This is the (read-only) software version of the Authorize.Net payment Gateway.
Merchant ID	Enter the IDentification number that you received from Authorize.Net.
Merchant Transaction Key	Enter the transaction key exactly as you received it from Authorize.Net. The transaction key is similar to a password. The Authorize.Net gateway uses the transaction key to authenticate transactions.

Table 8-1 CREDIT CARD

LABEL	DESCRIPTION
Market Type	This is the business type of your hot spot. Enter the market type value that you received from Authorize.Net. The market type value that Authorize.Net tells you depends on what type you applied for.
Device Type	This is the type of device that you are using to connect to the payment gateway (the ZyAIR B-4000 is type 5 at the time of writing).
Payment Gateway	Enter the address of the Authorize.Net gateway. The default value is “https://cardpresent.authorize.net/gateway/transact.dll”.
Email Additional Information	Select this check box to have the ZyAIR e-mail the subscriber the information that you specify in the following fields.
Merchant Name	Select this check box to have the ZyAIR include the company name in the e-mail that it sends to the subscriber. Enter the company name (up to 40 characters) in the field provided.
Username and Password	Select this check box to have the ZyAIR e-mail the subscriber the subscriber user name and password.
Usage Time	Select this check box to have the ZyAIR e-mail the subscriber the amount of usage time purchased.
Credit Card icons to be displayed on the login page	Select the check box(es) of the credit card icon(s) that you want the ZyAIR to display on the subscriber login page.
Apply	Click **Apply** to save your settings to the ZyAIR.

Part III:

Advanced Subscriber Account Management

This part covers the **ADVANCED KEYPAD**, **CUSTOMIZATION**, **PASS THROUGH**, **FILTERING** and **SHARE** screens.

Chapter 9
Keypad

This chapter shows you how to set up the optional keypad for the exclusive printer.

9.1 About the Keypad

You can use an optional PS/2 numeric keypad with the exclusive printer. Use this screen to define functions for the keys.

This function only works with the three-button printer

9.2 Keypad Settings

Click **ADVANCED** and **KEYPAD** to display the screen as shown next.

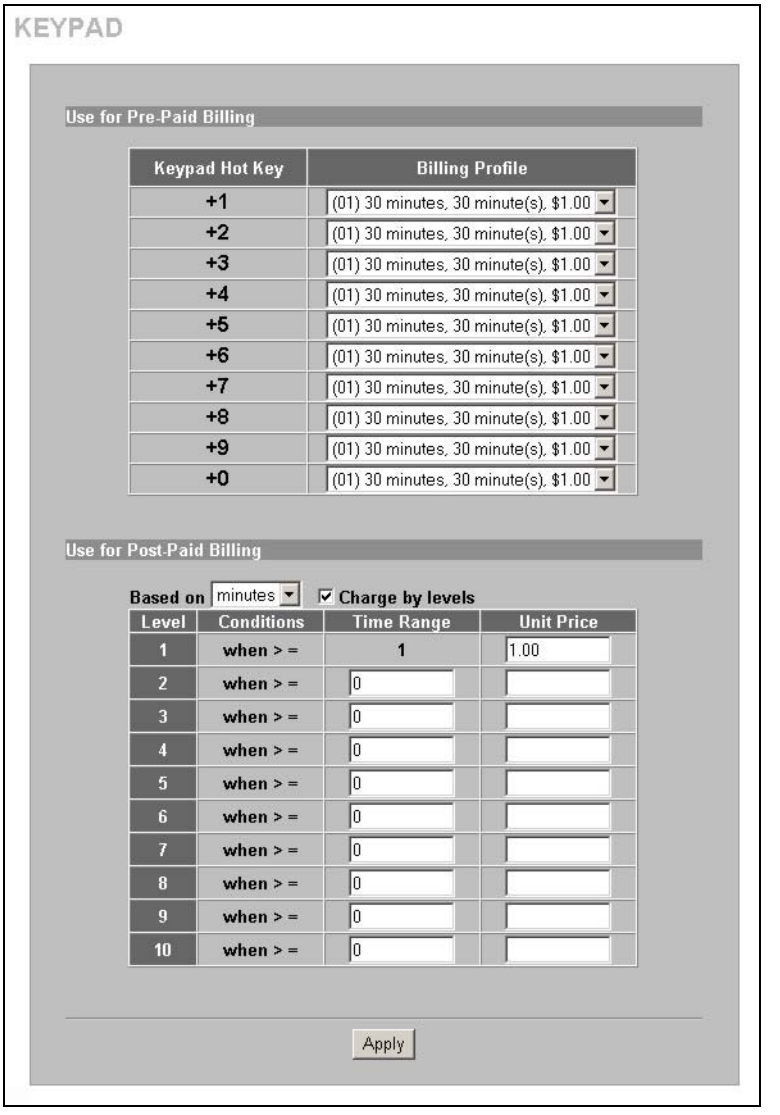


Figure 9-1 KEYPAD

The following table describes the labels in this screen.

Table 9-1 KEYPAD

LABEL	DESCRIPTION
Use for Pre-Paid Billing	The system provides ten user definable hot keys through the use of the + Key plus the 1 through 0 keys across the top of the keypad.
Keypad Hot Key	+1~+0 This is the combination hot key for a keypad application.
Billing Profile	Select the billing profile that you want to assign to the combination hot key. Use the **Billing** screen to configure and activate billing profiles. Only active billing profiles display here for you to choose from.
Use for Post-Paid Billing	Use the following fields to define the basic charge levels and rates for accounts.
Base on	Select the billing time unit from the drop-down list box.
Charge by levels	Use this field to enable or disable the charge by levels function. See the *Accounting* chapter for details on the charge by levels function.
Level	These are the read-only level numbers of the charges.
Time Range	Enter the number of time units (defined in the **Base on** field) for this charge level.
Unit Price	Enter each level's charge per time unit.
Apply	Click **Apply** to save the changes.

9.3 Keypad Configuration Examples

These sections explain how to configure the ZyAIR for use with a PS/2 keypad.

9.3.1 Keypad with Pre-Paid Billing Example

The following is an example of how to configure the ZyAIR to use a PS/2 keypad for pre-paid billing.

Step 1. Click **ADVANCED**, **BILLING**.

Step 2. Select **Pre-Paid** and click **Apply**.

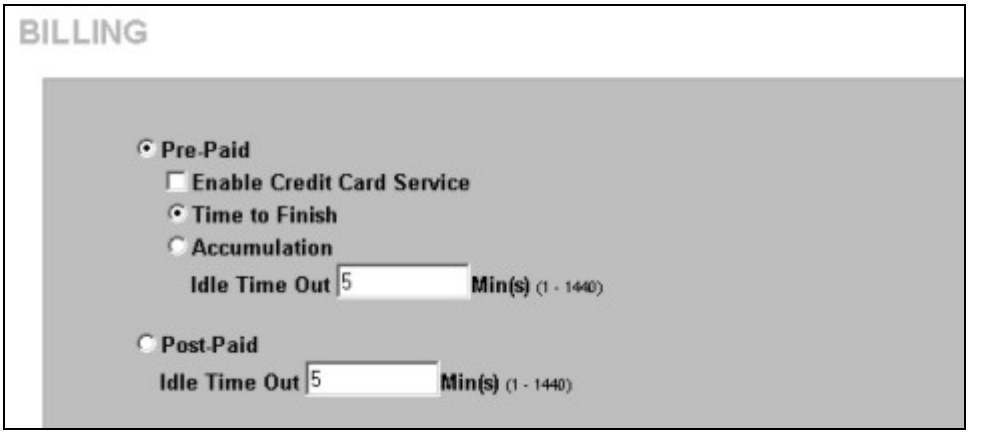


Figure 9-2 Select Pre-Paid Billing

Step 3. Click **ADVANCED**, **KEYPAD**.

Step 4. Define your pre-paid billing profiles and click **Apply**.

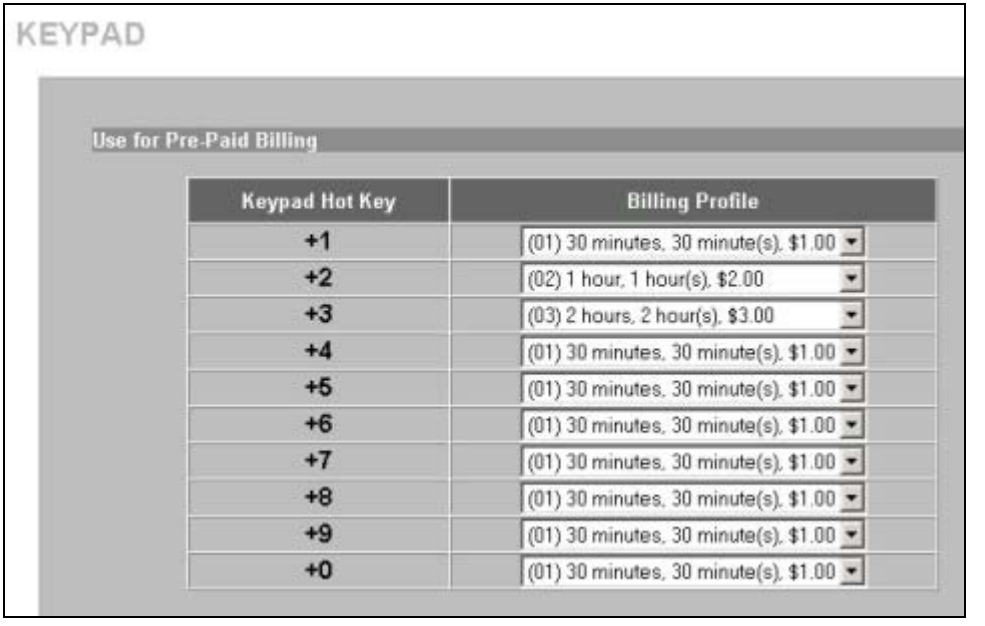


Figure 9-3 Define Pre-Paid Billing Profiles

Step 5. Use the keypad to create subscriber accounts. Press the keypad hot key and then [ENTER] to generate a new subscriber account and print the account information.

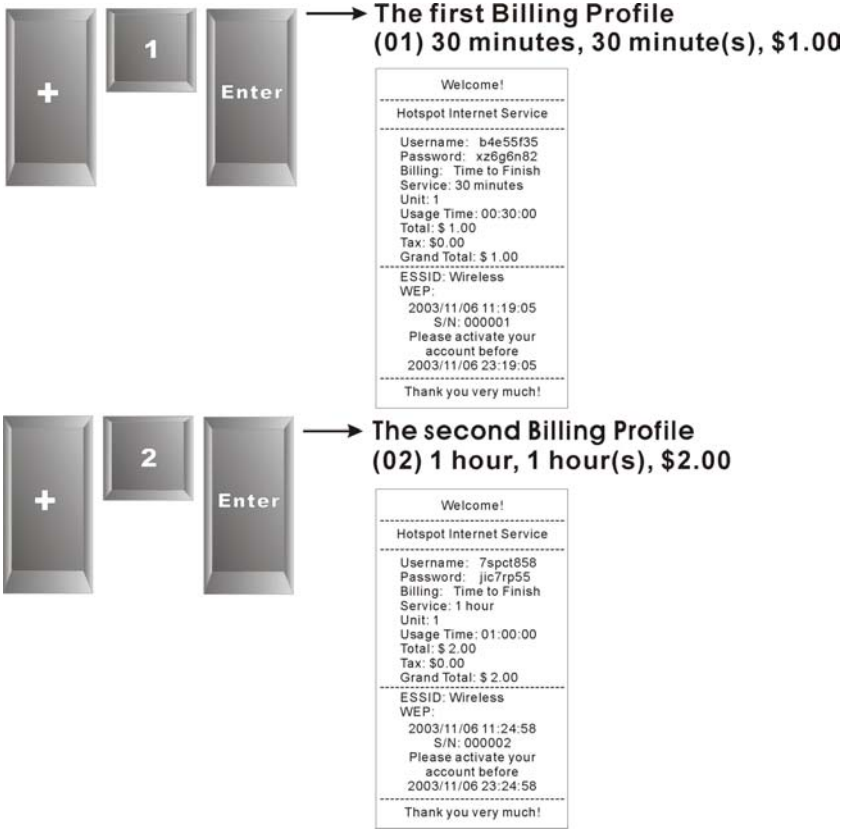


Figure 9-4 Billing Profiles 1 and 2 Examples

9.3.2 Keypad with Post-Paid Billing Example

The following is an example of how to configure the ZyAIR to use a PS/2 keypad for post-paid billing.

Step 1. Click **ADVANCED**, **BILLING**.

Step 2. Select **Post-Paid** and click **Apply**.

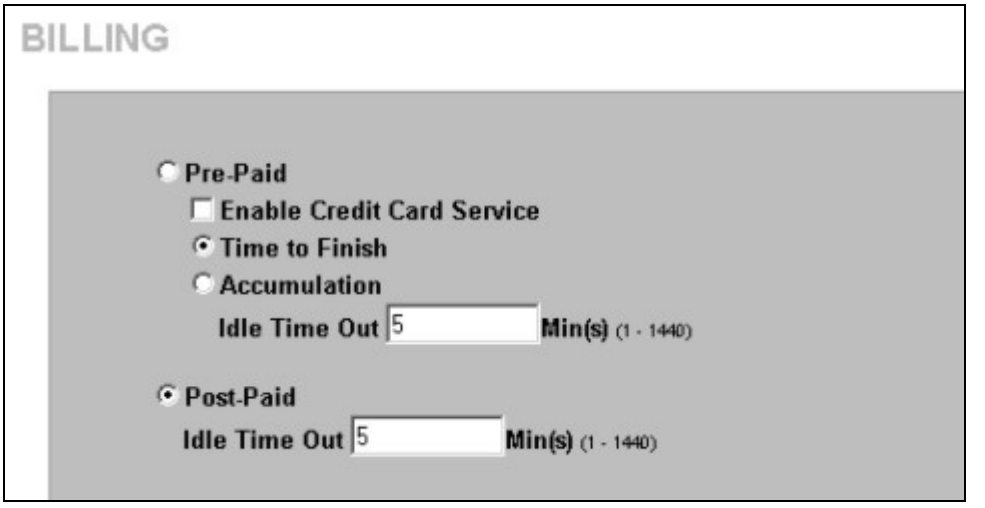


Figure 9-5 Select Post-Paid Billing

Step 3. Click **ADVANCED**, **KEYPAD**.

Step 4. Define your post-paid billing plan and click **Apply**.

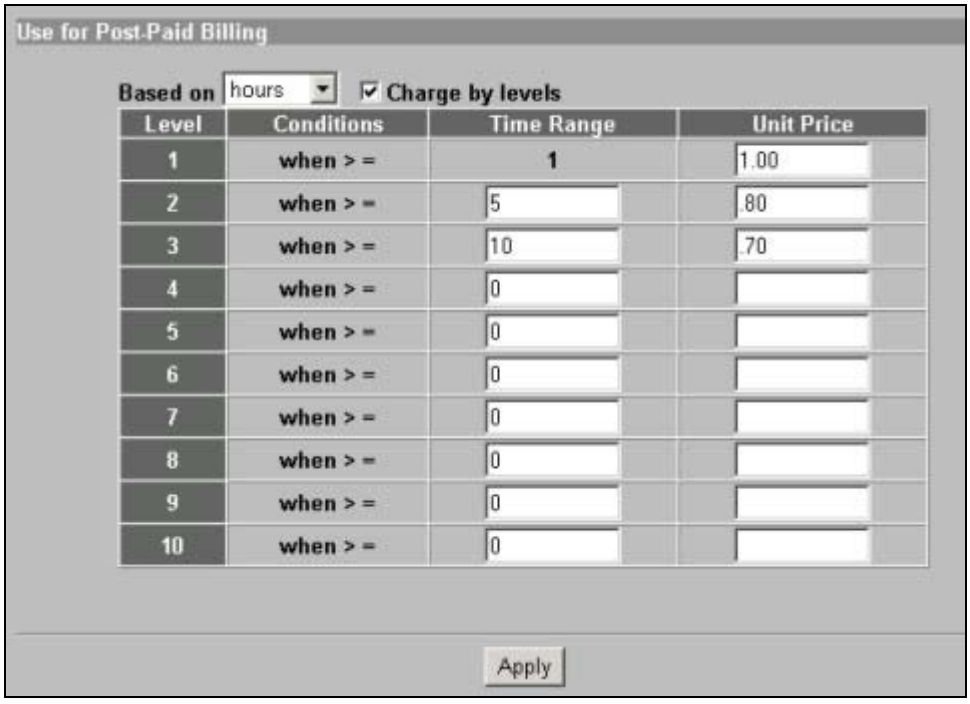


Figure 9-6 Define Post-Paid Billing Plan

Step 5. Use the keypad to create subscriber accounts. Press [ENTER] to generate a new subscriber account and print the account's information. The account information includes a serial number, password and the time the account was created.

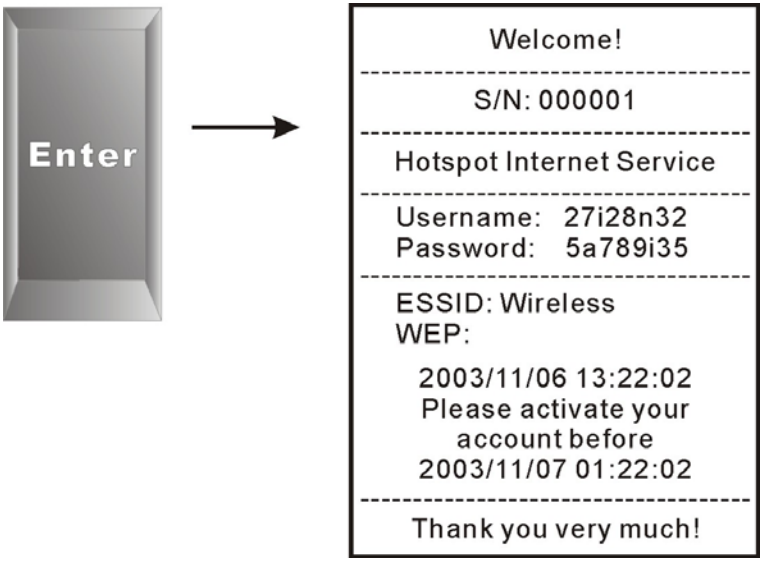


Figure 9-7 Post-Paid Account Printout Example

Step 6. When a subscriber is done using the Internet service, press the following to print a bill.

a. *
b. serial number
c. [ENTER]

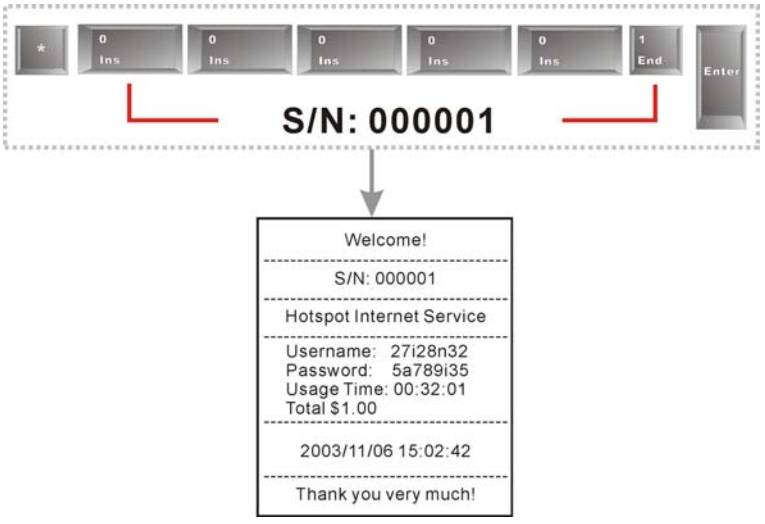


Figure 9-8 Post-Paid Account Bill Printout Example

Chapter 10 Customization

This chapter shows you how to customize the subscriber interface.

10.1 About the Customization Screens

Use these screens to tailor what displays on the subscriber interface. You can configure the subscriber login screen, which logo displays; an information window, the account printouts and the credit card billing interface.

10.2 About the Login Page Screen

When subscriber authentication is activated in the **Authentication** screen, the subscriber login screen is the first screen that all subscribers see when trying to access the Internet. You can configure walled garden web addresses for web sites that all subscribers are allowed to access without logging in (refer to the chapter on advertisement links and walled garden).

The ZyAIR provides different formats in which you can customize the login screen: **Standard**, **Redirect**, **Advanced** and **Frame**.

10.3 Customizing the Subscriber Login Screen

To customize the subscriber login screen, click **ADVANCED**, **CUSTOMIZATION** and **Login Page** to display the screen as shown next.

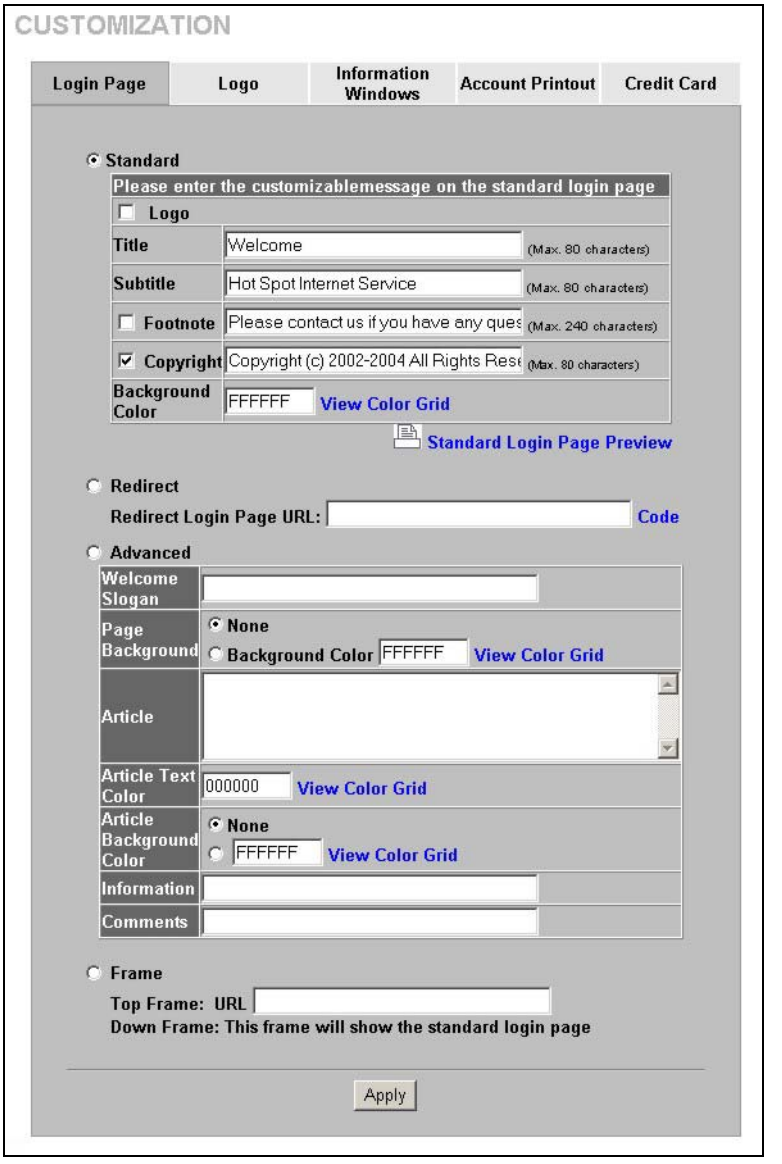


Figure 10-1 Login Page

10.3.1 Standard Subscriber Login Screen

The standard subscriber login screen is the ZyAIR's pre-configured, default simple login screen. In **Login Page**, select **Standard**.

Figure 10-2 Login Page: Standard

Table 10-1 Login Page: Standard

LABEL	DESCRIPTION
Logo	Select this check box to display your logo on the on the subscriber login screen. See section *10.4* for how to upload a logo file.
Title	Enter the title name (up to 80 characters) of the subscriber login page.
Subtitle	Enter the subtitle name (up to 80 characters) of the subscriber login page.
Footnote	Select the check box to add a footnote to the subscriber login page. Enter the footnote (up to 240 characters) in the field provided.
Copyright	Select the check box to add copyright information to the bottom of the subscriber login page. Enter the copyright information (up to 80characters) in the field provided.
Background Color	Enter a hexadecimal number to set the color of the login screen background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Standard Login Page Preview	Click this link to preview the standard login screen in a new browser window.

The following figure shows an example of what a subscriber sees when logging in.

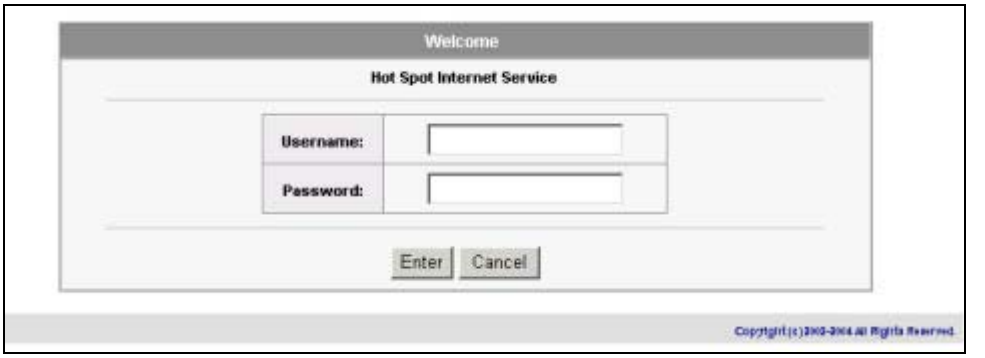


Figure 10-3 Login Page Example: Standard

10.3.2 Redirect Subscriber Login Screen

You can set the ZyAIR to redirect the subscribers to another login screen. This allows you to use your own customized login screen that you have created with a website-design tool. This gives you the ability to use a company login page and/or add multimedia features such as flash.

In the **Login Page** screen, select **Redirect**.

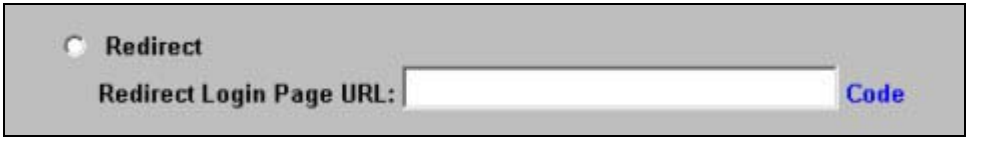


Figure 10-4 Login Page: Redirect

The following table describes the related labels.

Table 10-2 Login Page: Redirect

LABEL	DESCRIPTION
Redirect	Select this option to direct the subscriber to another login screen.
Redirect Login Page URL	Specify the web site address to which the ZyAIR directs the subscribers for logins. The web site must be on the WAN.
Code	Click **Code** to display the source code of the web page you specify above (see *Figure 10-5*). The redirect subscriber login screen must include the HTML source code in the default sample page in order for the subscriber login screen to send the subscribers' usernames and passwords to the ZyAIR.

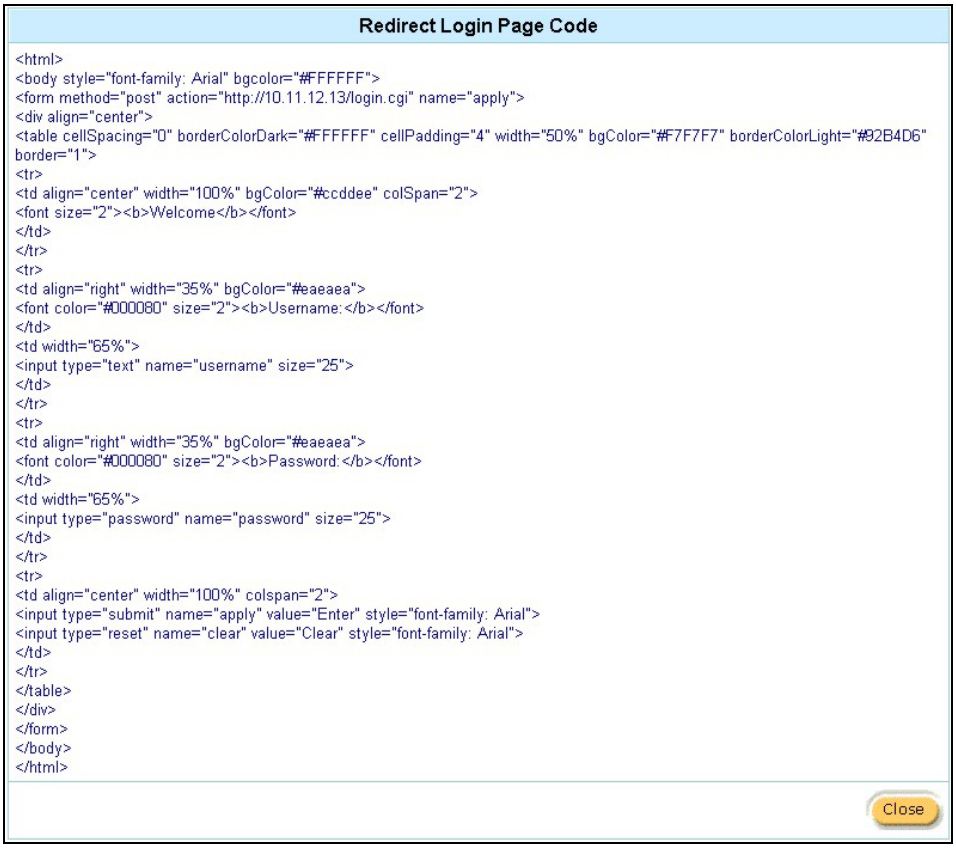


Figure 10-5 Login Page: Redirect Code

10.3.3 Advanced Subscriber Login Screen

Use the **Advanced** login screen option to customize a login screen where you can create a welcome slogan and add advertising information.

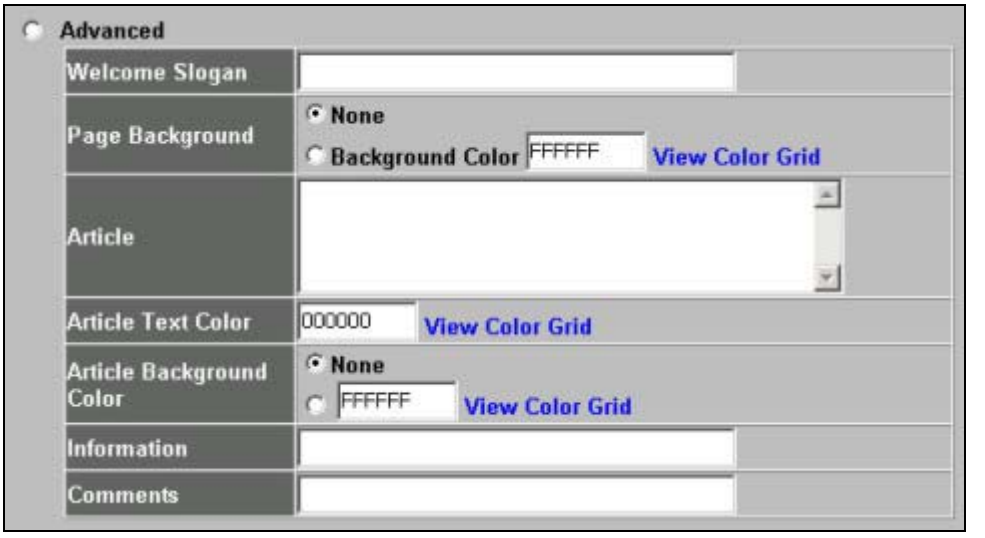


Figure 10-6 Login Page: Advanced

The following table describes the related labels.

Table 10-3 Login Page: Advanced

LABEL	DESCRIPTION
Advanced	Select this option to set the ZyAIR to display the advanced subscriber login screen.
Welcome Slogan	Enter a welcome message (up to 80 characters long) in the text box provided.
Page Background	Select **None** to set the background color of the login screen to white (the default). Select **Background Color** to set the color of the login screen background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Article	Enter a block of text (up to 1024 characters long) in the text box. This is useful for advertisements or announcements.
Article Text Color	Select **None** to set the article text color of the login screen to white (the default). Select and set the color of the article text block background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.

Table 10-3 Login Page: Advanced

LABEL	DESCRIPTION
Article Background Color	Select **None** to set the article background color of the login screen to white (the default). Select the other radio button to set the color of the login screen's article background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Information	Enter information such address and telephone or fax numbers in the text box provided. Up to 80 characters allowed.
Comments	Enter any comments (up to 80 characters long) in the text box provided.

The web-friendly color sets are displayed in the figure shown.

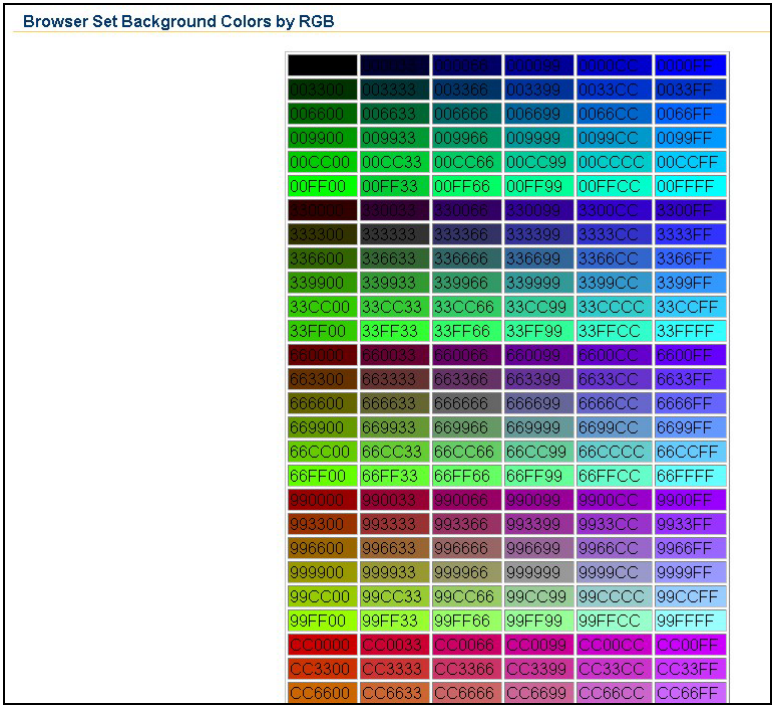


Figure 10-7 Login Page: Color Grid

The following figure shows an advanced subscriber login screen example.

Figure 10-8 Subscriber Login Screen Example: Advanced

10.3.4 Framed Subscriber Login Screen

The **Frame** login screen splits the login screen into two frames: top and bottom. You can specify a web site to be displayed in the top frame with the user name and password prompt displayed in the bottom frame. The frame login screen is useful for you to link to a web site (such as the company web site) as your welcome screen. In addition, you can externally design a web page with images and/or advanced multimedia features.

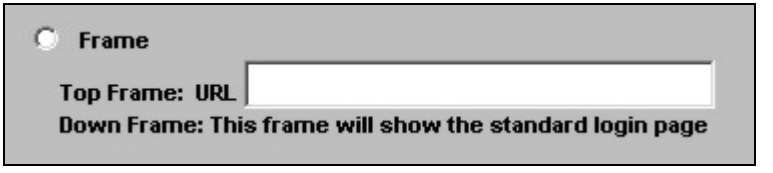


Figure 10-9 Subscriber Login Screen: Frame

The following table describes the related labels.

Table 10-4 Subscriber Login Screen: Frame

LABEL	DESCRIPTION
Frame	Select this option to configure and set the ZyAIR to display the subscriber login screen in two frames.
Top Frame	Enter a web site address in the **URL Link** field, for example, http://www.zyxel.com.
Down Frame	The bottom frame displays the standard subscriber login page.

The following figure shows a framed subscriber login screen example.

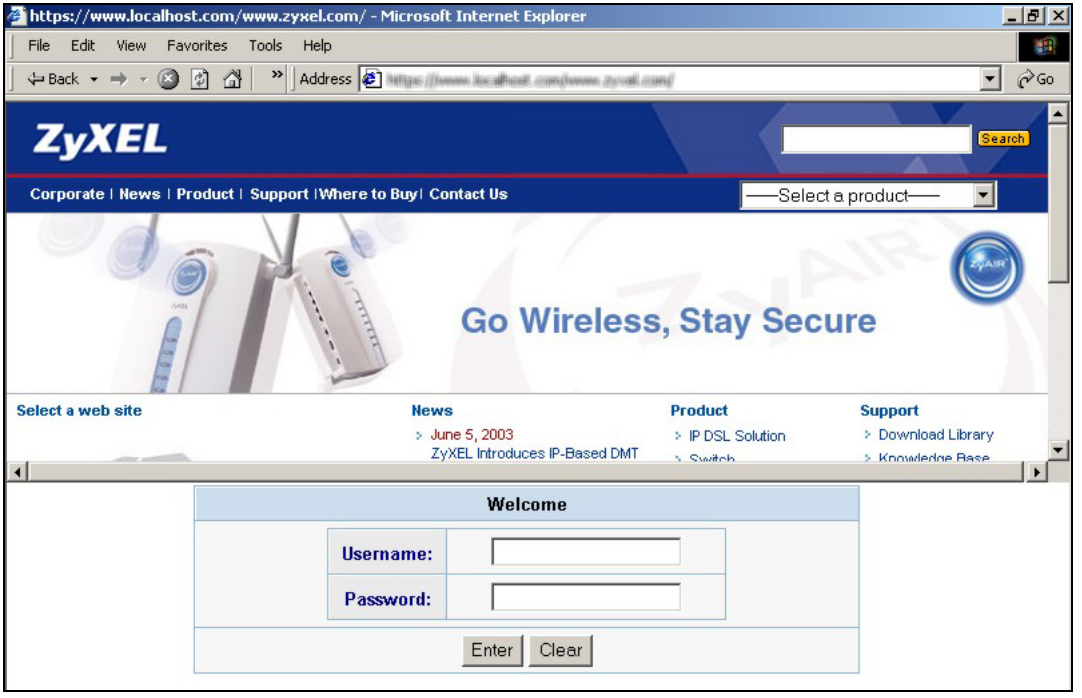


Figure 10-10 Subscriber Login Screen Example: Frame

10.4 Adding a Logo

This function allows you to upload a file containing your logo. The logo can be shown on the standard login page and the account printout when printing with a network-connected printer.

To upload your logo file, click **ADVANCED**, **CUSTOMIZATION** and **Logo** to display the screen as shown next.

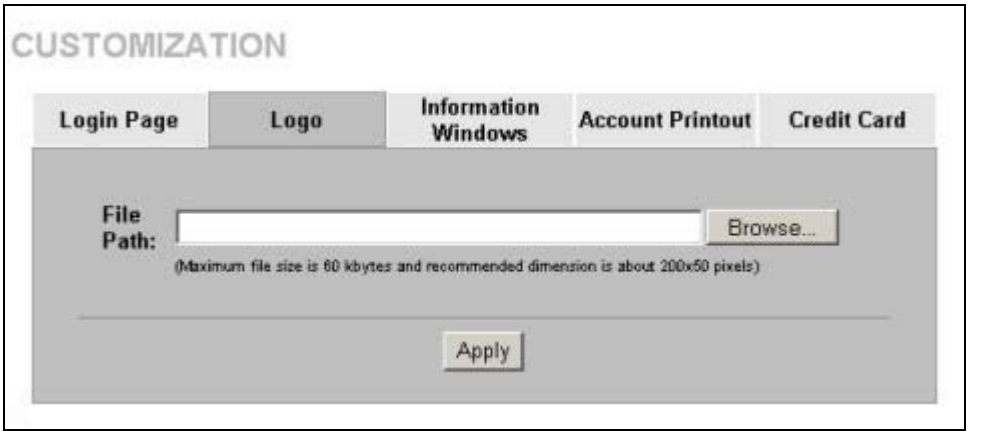


Figure 10-11 Logo

The following table describes the labels in this screen.

Table 10-5 Logo

LABEL	DESCRIPTION
File Path	Enter the file pathname of the logo file or click **Browse** to search for it.
Apply	Click **Apply** to upload your logo file to the ZyAIR.

10.5 About the Information Window

You can set the ZyAIR to display an information window after a subscriber has successfully logged in. This information window shows the amount of time a subscriber has used or the time the subscriber still has to access the Internet.

The subscriber information window varies depending on the account type and billing configuration you set on the ZyAIR.

The information window displays the amount of time used for Internet access on a super subscriber account. With other types of account, the information window displays the amount of time a subscriber still has to use for Internet access.

When you set the system to allow accounts to be replenished, the information window displays a **Replenish** button.

When you set the billing type to accumulation, the information window displays a **Logout** button.

10.5.1 Customizing the Information Window

Click **ADVANCED**, **CUSTOMIZATION** and **Information Window** to display the screen as shown next.

To display the information window on the subscriber's computer after a successful login, select the **Display Information Window once after a subscriber logs in successfully** check box.

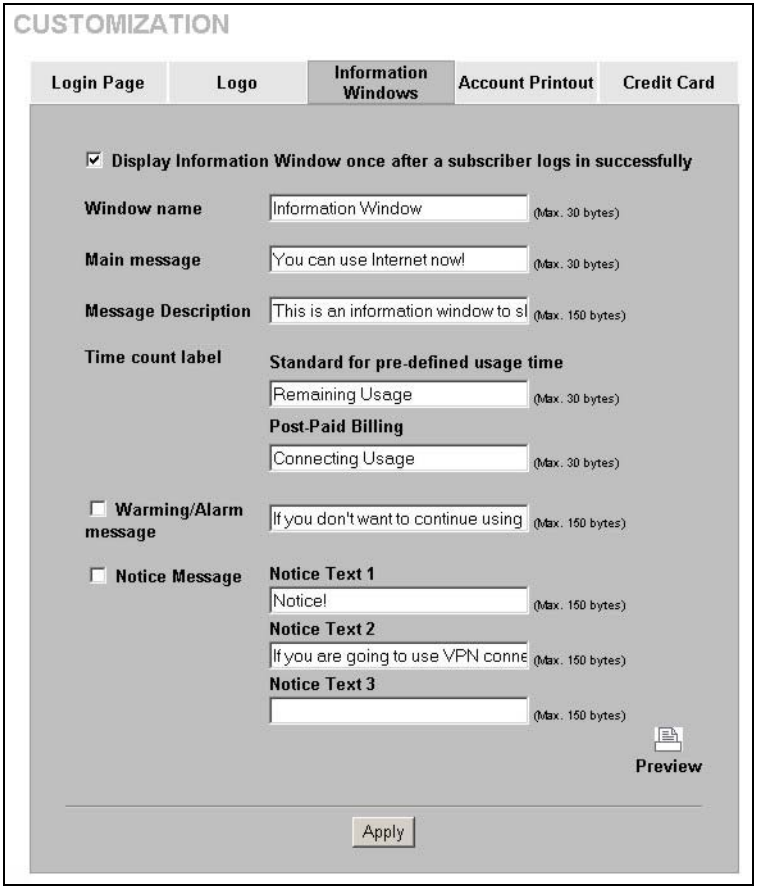


Figure 10-12 Customization: Information Window

The following table describes the labels in this screen.

Table 10-6 Customization: Information Window

LABEL	DESCRIPTION
Window name	Enter a descriptive name (up to 30 characters) as the title of the window.
Main message	Enter a short message (up to 30 characters).
Message Description	Enter a short description about the information window.
Time count label	**Standard for pre-defined usage time** -Enter the label for the field displaying the remaining time. This field displays when the ZyAIR is set to use pre-paid billing. **Post-Paid Billing** -Enter the label for the field displaying the amount of time used. This field displays when the ZyAIR is set to use post-paid billing.
Warning/Alarm Message	Select this check box to display the warning message that you enter in the text box provided.
Notice Message	Select this check box to display any additional message(s) that you enter in the text box(es) provided. You can specify up to three additional messages (such as discount information) in the information window.
Preview	Click **Preview** to display a preview of the information window.
Apply	Click **Apply** to save the changes.

10.6 About the Account Printout

After you have created the subscriber accounts, you can print out the account information.

10.6.1 Customizing the Account Printout

To customize the account printout, click **ADVANCED**, **CUSTOMIZATION** and **Account Printout** to display the screen as shown.

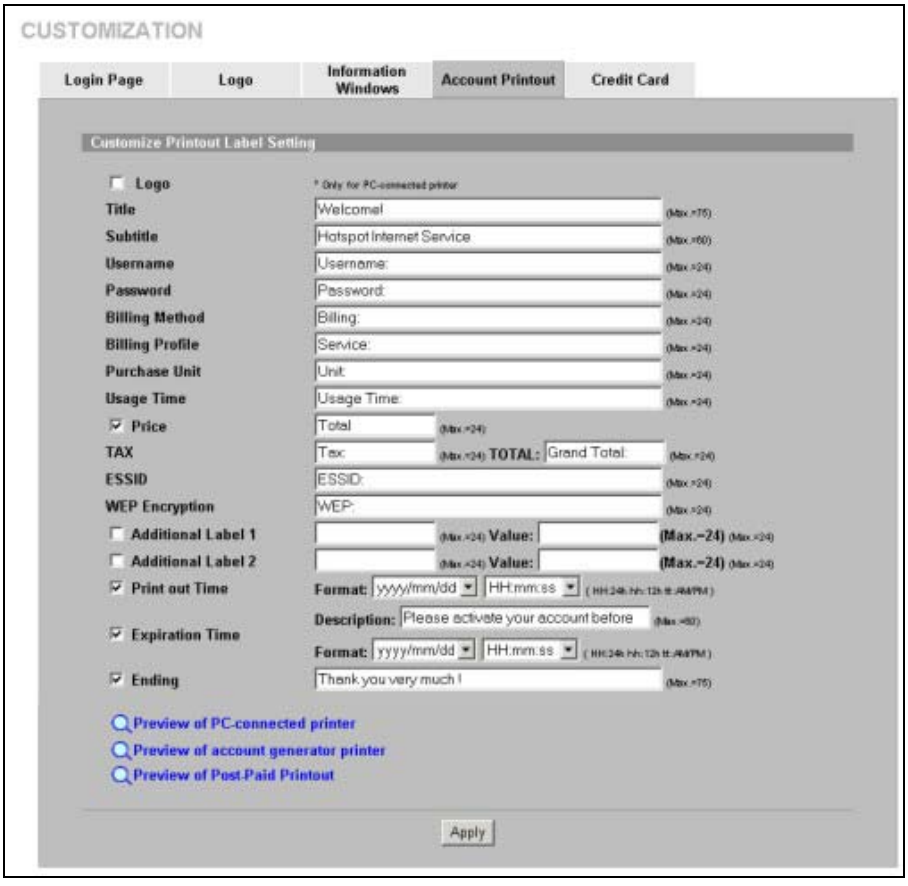


Figure 10-13 Account Printout

The following table describes the labels in this screen.

Table 10-7 Account Printout

LABEL	DESCRIPTION
Logo	Select this check box to print your logo on the account statement when you use a network-connected printer. See section *10.4* for how to upload a logo file.
Title	Enter a title (up to 75 characters) for the printout.
Subtitle	Enter a subtitle (up to 80 characters) for the printout.

Table 10-7 Account Printout

LABEL	DESCRIPTION
Username	Enter the label name for the field displaying the account username.
Password	Enter the label name for the field displaying the account password.
Billing Method	Enter the label name for the field displaying the method for billing.
Billing Profile	Enter the label name for the field displaying the name for the billing profile used.
Purchase Unit	Enter the label name for the field displaying the number of time units purchased.
Usage Time	Enter the label name for the field displaying the amount of time an account is allowed for Internet access.
Price	Select this check box to display the specified label name for the field displaying the price.
Tax	Enter a label name for the field displaying the tax.
Total	Enter a label name for the field displaying the sum of the price and the tax.
ESSID	Type a label name for the field displaying the wireless LAN's Extended Service Set Identifier (**ESSID**).
WEP	Type a label name for the field displaying the Wired Equivalent Privacy (**WEP Encryption**) key.
Additional Label 1.. 2	Select this check box to display the specified label name(s) for the field(s) displaying any additional information.
Print out Time	Select this check box to display the time an account is printed out. Select date and time formats from the drop-down list boxes.
Expiration Time	Select this check box to display the time an account expires. Enter an explanation for the subscriber about the account's expiration. Select date and time formats from the drop-down list boxes.
Ending	Select this check box to display a message at the end of the printout. Enter the message (up to 75 characters) in the text box provided.
Preview of PC-connected printer	Click **Apply** to save your changes and then click this link to display a preview of an account printout, as it would print on a printer connected to a network computer.
Preview of account generator printer	Click this link to display a preview of an account printout, as it would print on an external account generator printer (or the statement printer).

Table 10-7 Account Printout

LABEL	DESCRIPTION
Preview of Post-Paid Printout	Click this link to display a preview of a post-paid account printout.
Apply	Click **Apply** to save the changes.

The following figures show account printout examples.

Figure 10-14 Preview of PC-connected Printer Example

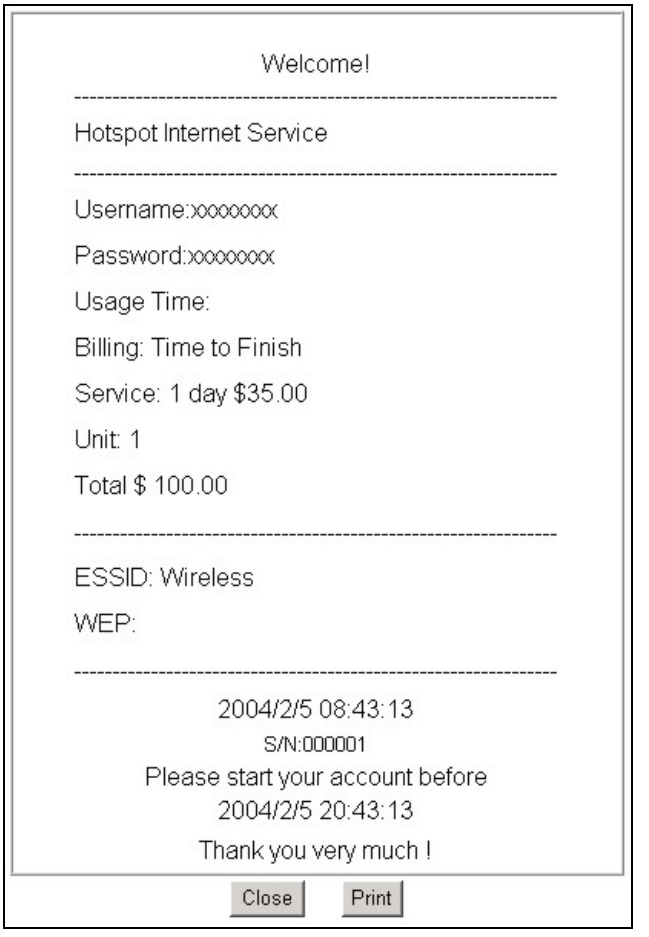


Figure 10-15 Preview of Account Generator Printer Example

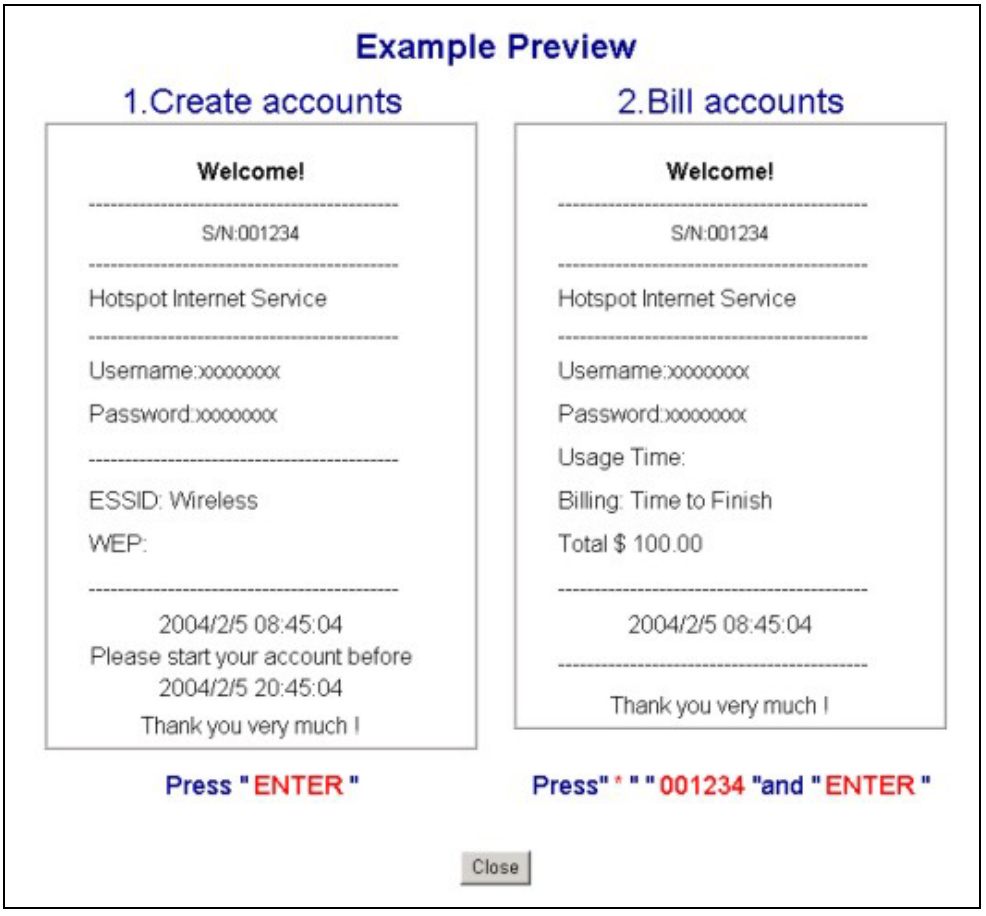


Figure 10-16 Preview of Post-Paid Printout Example

10.7 Customizing the Credit Card

When you configure the ZyAIR to use credit card billing, you can use this page to customize the subscriber billing interface. Click **ADVANCED**, **CUSTOMIZATION** and **Credit Card** to display the screen as shown.

10.7.1 Credit Card Standard Login Page

Use this section to customize the credit card message that displays on the standard login page.

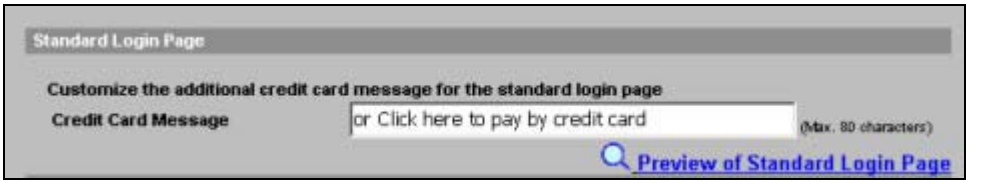


Figure 10-17 Credit Card: Standard Login Page

The following table describes the labels in this section.

Table 10-8 Credit Card: Standard Login Page

LABEL	DESCRIPTION
Standard Login Page	Enter the credit card message that you want to display on the standard login page. The message you configure here only displays on the standard login page when you configure and enable credit card service.
Preview of Standard Login Page	Click this link to display a preview of the standard login page.

The following figure shows an example of the standard login page with the credit card option.

Figure 10-18 Credit Card Standard Login Page Example

10.7.2 Credit Card Service Selection Page

Use this section to customize the credit card billing interface that displays on the subscriber's screen.

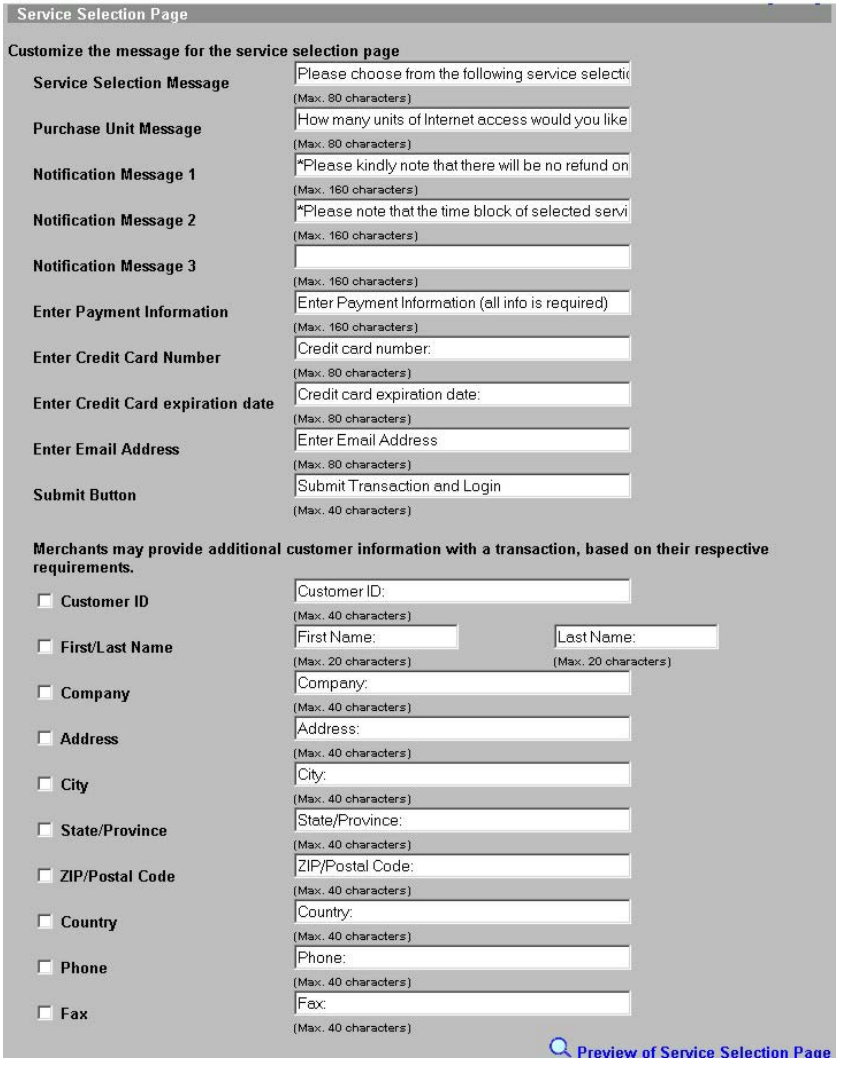


Figure 10-19 Credit Card Service Selection Page

The following table describes the labels in this section.

Table 10-9 Credit Card Service Selection Page

LABEL	DESCRIPTION
Service Selection Message	Enter a message to instruct the subscribers to select a billing profile. Use the Billing screen to configure and activate billing profiles. Only active billing profiles display on the subscriber's screen.
Purchase Unit Message	Enter a message to instruct the subscribers to select the number of time units to purchase.
Notification Message (1-3)	Enter an additional message(s) regarding the purchase of Internet access. For example, you may enter a refund policy.
Enter Payment Information	Enter a message to instruct the subscribers to provide the required payment information.
Enter Credit Card Number	Enter a label name for the field where the subscriber enters the credit card number.
Enter Credit Card expiration date	Enter a label name for the field where the subscriber enters the credit card's expiration date.
Enter Email Address	Enter a label name for the field where the subscriber enters an e-mail address.
Submit Button	Enter a label name for the button the subscriber clicks to submit the transaction information.
Optional Information	You may select check boxes to display additional fields on the credit card billing interface that displays on the subscriber's screen.
Customer ID	Select this check box if you want the screen to display a customer ID field. A customer with an Authorize.net-issued ID can enter it in the field. Enter the label name for the field that requests the subscriber's ID.
First/Last Name	Select this check box if you want the screen to display the first and last name fields. Enter the label names for the fields that request the subscriber's first and last name.
Company	Select this check box if you want the screen to display a company field. Enter the label name for the field that requests the name of the subscriber's company.
Address	Select this check box if you want the screen to display an address field. Enter the label name for the field that requests the subscriber's address.
City	Select this check box if you want the screen to display a city field. Enter the label name for the field that requests the name of the city where the subscriber lives.

Table 10-9 Credit Card Service Selection Page

LABEL	DESCRIPTION
State/Province	Select this check box if you want the screen to display a state or province field. Enter the label name for the field that requests the subscriber's state or province.
ZIP/ Postal Code	Select this check box if you want the screen to display a zip or postal code field. Enter the label name for the field that requests the subscriber's zip or postal code.
Country	Select this check box if you want the screen to display a country field. Enter the label name for the field that requests the subscriber's country.
Phone	Select this check box if you want the screen to display a phone number field. Enter the label name for the field that requests the subscriber's phone number.
Fax	Select this check box if you want the screen to display a fax number field. Enter the label name for the field that requests the subscriber's fax number.
Preview of Service Selection Page	Click this link to display a preview of the credit card service selection page that will display on the subscriber's screen.

The following figure shows an example preview of the credit card service selection page.

Figure 10-20 Credit Card Service Selection Page Preview

10.7.3 Credit Card Successful Page

Use this section to customize the page that displays on the subscriber's screen if an attempt to use a credit card is successful.

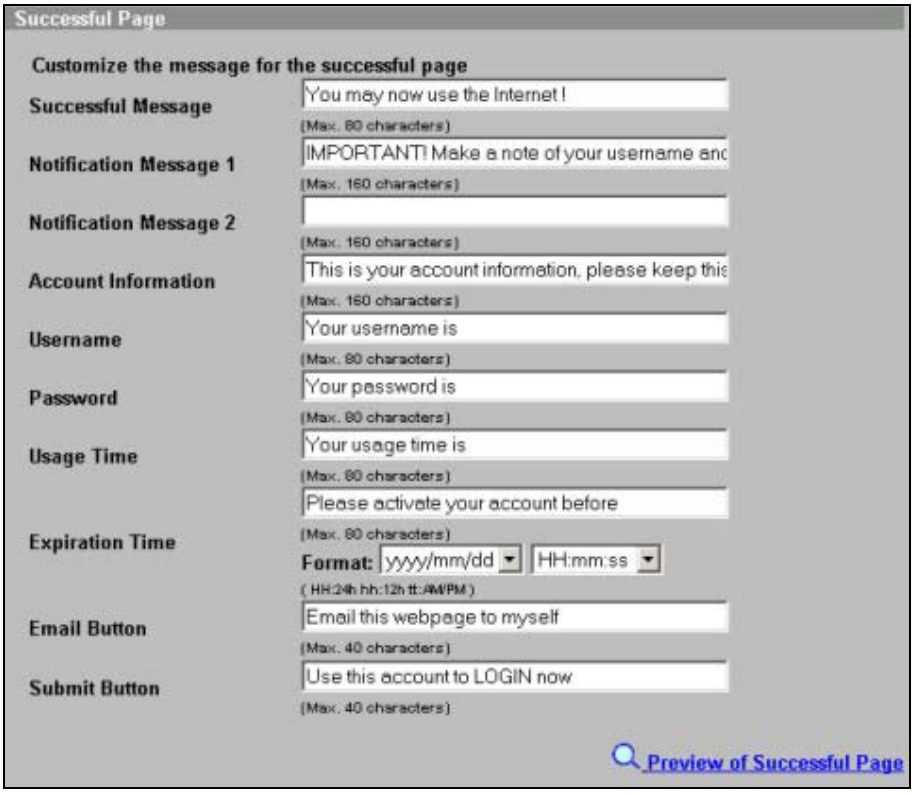


Figure 10-21 Credit Card Successful Page

The following table describes the labels in this section.

Table 10-10 Credit Card Successful Page

LABEL	DESCRIPTION
Successful Message	Enter a message to tell the subscriber that the online credit card transaction was successful.
Notification Message (1-2)	Enter an additional message(s) regarding the subscriber's use of the purchased Internet access.
Account Information	Enter a message to tell the subscriber about the account information in the following fields.
Username	Enter a label name for the field that displays the subscriber's user name.

Table 10-10 Credit Card Successful Page

LABEL	DESCRIPTION
Password	Enter a label name for the field that displays the subscriber's password.
Usage Time	Enter a label name for the field that displays the subscriber's purchased period of Internet access.
Expiration Time	Enter the label name for the field displaying when the account expires. Select date and time formats from the drop-down list boxes.
Email Button	Enter a label name for the button the subscriber can click to send a copy of the account information to the subscriber's e-mail account.
Submit Button	Enter a label name for the button the subscriber clicks to log into the account.
Preview of Successful Page	Click this link to display a preview of the credit card transaction successful page that will display on the subscriber's screen.

The following figure shows an example preview of the credit card transaction successful page.

Figure 10-22 Credit Card Successful Page Preview

10.7.4 Credit Card Fail Page

Use this section to customize the page that displays on the subscriber's screen if an attempt to use a credit card fails.

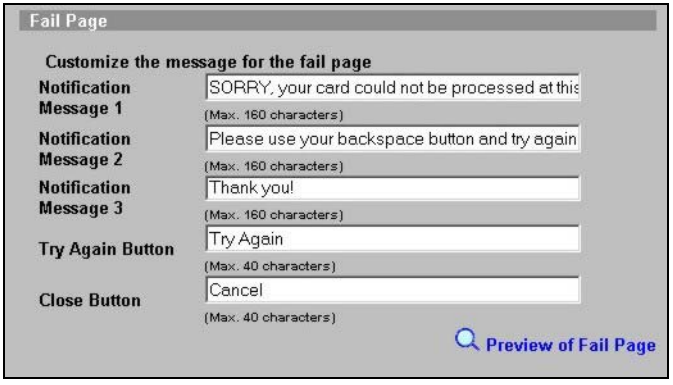


Figure 10-23 Credit Card Service Fail Page

The following table describes the labels in this section.

Table 10-11 Credit Card Service Fail Page

LABEL	DESCRIPTION
Notification Message (1-3)	Enter a message(s) to tell the subscriber that the online credit card transaction failed and how to try again.
Try Again Button	Enter a label name for the button that takes the subscriber back to the credit card service selection page.
Close Button	Enter a label name for the button that the subscriber can use to stop attempting to make a credit card transaction and close the credit card interface.
Preview of Fail Page	Click this link to display a preview of the credit card transaction failed page that will display on the subscriber's screen.

The following figure shows an example preview of the credit card transaction failed page.

Figure 10-24 Credit Card Failed Page Preview

Chapter 11
Pass Through

This chapter shows you how to specify devices that can have traffic pass through the ZyAIR.

11.1 About the Pass Through

You can set up two types of pass through on the ZyAIR: by device or by web site address.

You can set the ZyAIR to allow specific computers on the LAN (based on the IP or MAC address) to access the Internet without prompting for a user name and password. This feature is useful, for example, if you want to set up computers to provide free Internet access in the VIP room or for sponsors in events.

To allow global access to web sites, specify the web site address (by IP address or URL) that any user can access without logging in. This is similar to the walled garden feature, but without displaying the web site link(s) in the subscriber login screen. You have to inform the users about which web sites they can access for free.

11.2 Configuring Pass Through

To configure pass through on the ZyAIR, click **ADVANCED** and then **PASS THROUGH**.

Pass through has priority over filtering.

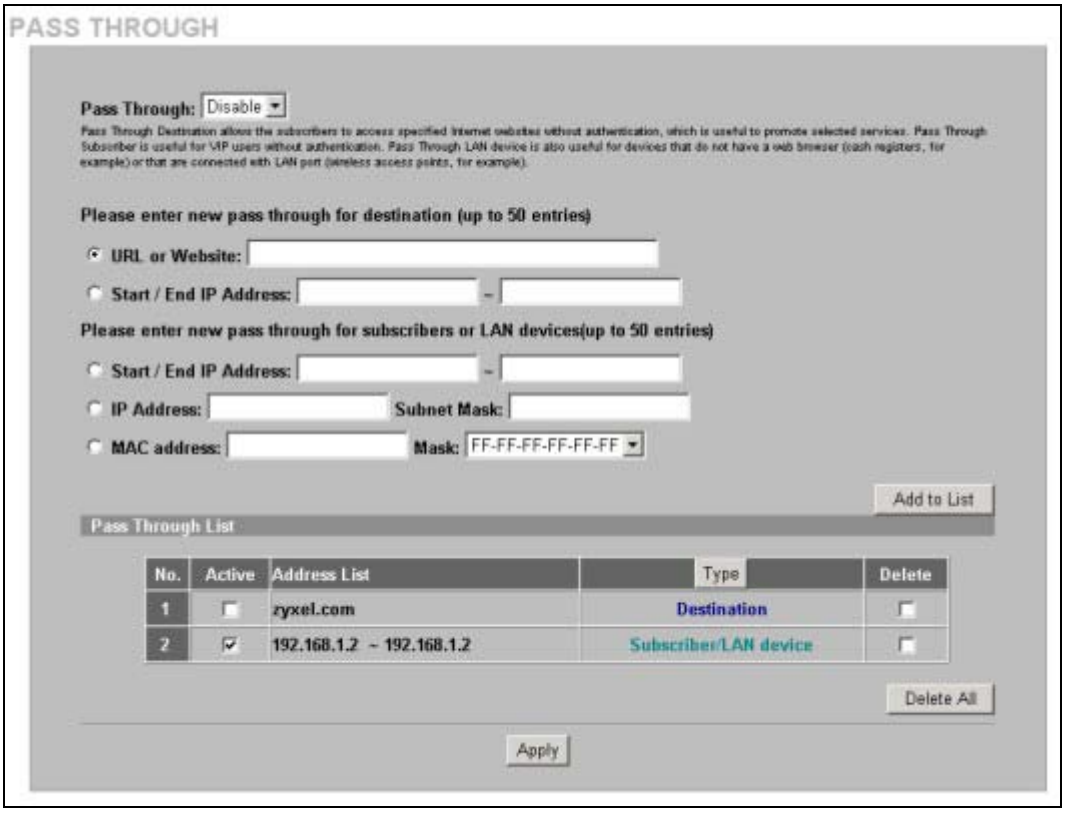


Figure 11-1 PASS THROUGH

The following table describes the labels in this screen.

Table 11-1 PASS THROUGH

LABEL	DESCRIPTION
Pass Through	Enable pass through to allow all users to access specific web sites (or IP addresses) and/or allow packets from specific computers to go through the ZyAIR without prompting for a user name and password.
Please enter new pass through for destination (up to 50 entries) The destinations should be on the WAN.	

Table 11-1 PASS THROUGH

LABEL	DESCRIPTION
URL or Website	Select this option to allow users to access a website without entering a user name or password. Enter the URL (up to 50 ASCII characters) of the web site to which you want to allow access.
Start / End IP Address	Select this option to allow users to access a range of IP addresses without entering a user name or password. Enter the beginning and ending IP addresses in dotted decimal notation.
Please enter new pass through for subscribers or LAN devices(up to 50 entries)	
Start / End IP Address	Select this option to allow packets from computers with a specific range of IP addresses to pass through the ZyAIR without entering a user name and password. Enter the beginning and ending IP addresses IP addresses in dotted decimal notation, for example, 192.168.1.10.
IP Address	Select this option to allow packets from a computer with a specific IP address to pass through the ZyAIR without entering a user name and password. You can specify a range of IP addresses on a network by specifying an IP address here and a subnet mask in the **Subnet Mask** field. Enter the IP address in dotted decimal notation, for example, 192.168.1.10.
Subnet Mask	Enter the subnet mask of the IP address that you entered in the **IP Address** field.
MAC Address	Select this option to allow packets from a computer with a specific MAC address to pass through the ZyAIR without entering a user name and password. Enter the MAC address of a computer (in 6 hexadecimal pairs separated by a hyphen "-", for example, 00-50-BA-8D-22-96).
Mask	Enter the subnet mask of the MAC address that you entered in the **MAC Address** field.
Add to List	Click this button to add the pass through entry you configured to the **Pass Through List**.
Pass Through List This table displays the device and web site address entries that you have set up on the ZyAIR.	
No.	This read-only field displays the index number of a pass through entry.

Table 11-1 PASS THROUGH

LABEL	DESCRIPTION
Active	Select this check box to turn on this pass through entry and allow access without a user name and password. Clear this check box to turn off this pass through entry and block access without a user name and password.
Address List	This read-only field displays the address(es) of a pass through entry.
Type	This read-only field displays “Destination” for a pass through entry based on a destination URL or IP address. The field displays “Subscriber/LAN device” for a pass through entry based on a LAN device or a subscriber’s computer. Click the column heading to sort the pass through entries by type (**Destination** or **Subscriber/LAN device**).
Delete	Select this check box(es) and click **Apply** to remove the pass through entry.
Delete All	Click this button to remove all of the pass through entries.
Apply	Click **Apply** to save the new settings.

Chapter 12
Filtering

This chapter shows you how to configure the ZyAIR's filter function.

12.1 About Filtering

Filtering allows you to block subscriber access to a list of destinations. This lets you block access to specific Internet websites or IP addresses. An example of what this would be useful for is blocking access to sites where subscribers would use large amounts of bandwidth for large file downloads or file sharing.

12.2 Configuring Filtering

To configure filtering on the ZyAIR, click **ADVANCED**, **FILTERING** to display the screen as shown next.

Pass through has priority over filtering.

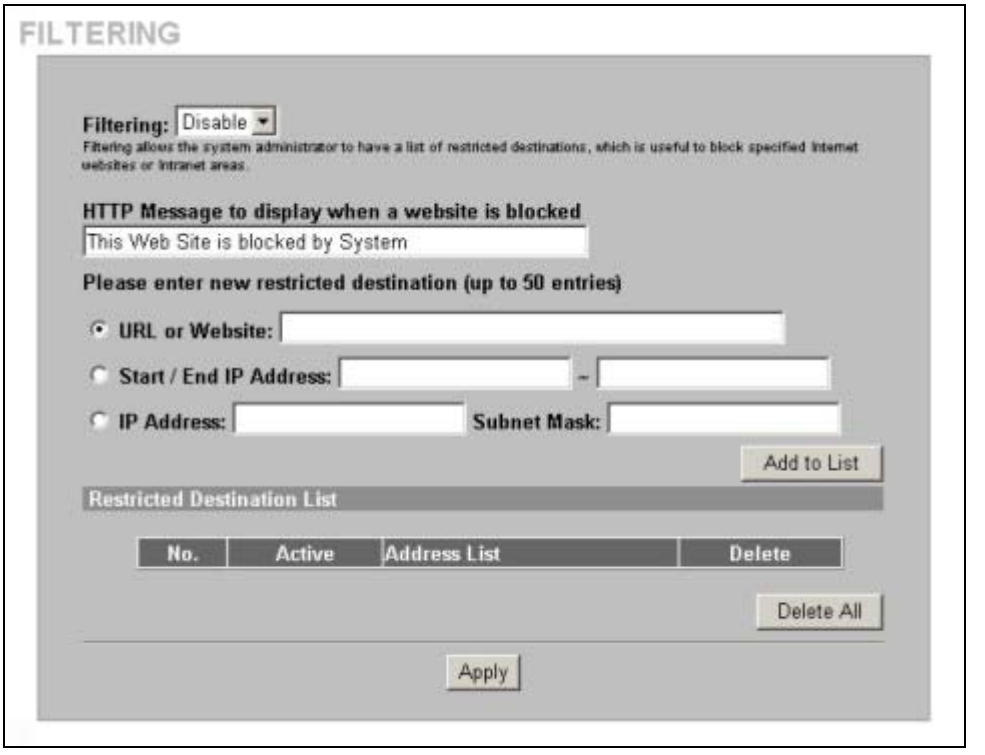


Figure 12-1 FILTERING

The following table describes the related labels.

Table 12-1 FILTERING

LABEL	DESCRIPTION
Filtering	Enable filtering to block subscriber access to specified Internet websites or IP addresses.
HTTP Message to display when a website is blocked	Enter a message to display on the subscriber's screen when the system blocks access to a website. The default message is "This Web Site is blocked by System".

Table 12-1 FILTERING

LABEL	DESCRIPTION
Please enter new restricted destination (up to 50 entries)	Use these fields to add to the list of forbidden destinations.
URL or Website	Enter the full URL of the website to which you want to block subscriber access for example, “http://www.yahoo.com”. You can use up to 200 characters.
Start / End IP Address	Enter the beginning and ending IP addresses of a range of IP addresses to which you want to block subscriber access.
IP Address	Enter an IP address to which you want to block subscriber access.
Subnet Mask	Enter the subnet mask of the IP address to which you want to block subscriber access.
Add to List	Click this button to add a new entry to the list of restricted destinations.
Restricted Destination List	This table lists Internet destinations to which the system is to block subscriber access.
No	This is the index number of a destination entry.
Active	Select this check box to block subscriber access to this destination.
Address List	This field displays the destination address(s).
Delete	Select this check box(es) and click **Apply** to remove the destination entry.
Delete All	Click this button to remove all of the destination entries.
Apply	Click **Apply** to save the new settings.

Chapter 13
Share

This chapter shows you how to configure the ZyAIR for the sharing of network devices.

13.1 About Share

The share function allows logged-in subscribers to share devices on the LAN. This is useful for allowing subscribers to use printers or servers.

13.2 Configuring Share

To configure sharing on the ZyAIR, click **ADVANCED**, **SHARE** to display the screen as shown next.

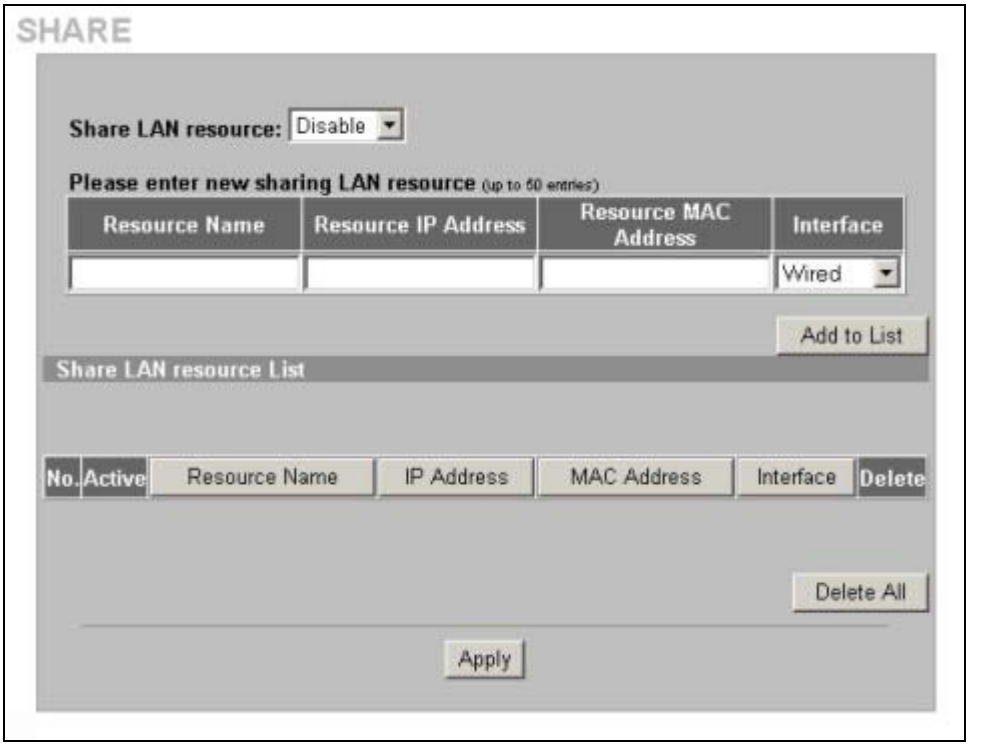


Figure 13-1 SHARE

The following table describes the related labels.

Table 13-1 SHARE

LABEL	DESCRIPTION
Share LAN resource	Enable the sharing of LAN resources to allow logged-in subscribers to access specific devices on the LAN. Disable the sharing of LAN resources to block logged-in subscribers from accessing devices on the LAN.
Resource Name	Enter the LAN device's name (up to 50 ASCII characters).
Resource IP Address	Enter the IP address of the LAN device.

Table 13-1 SHARE

LABEL	DESCRIPTION
Resource MAC Address	Enter the MAC address of the LAN device.
Interface	Select the ZyAIR's interface to which the LAN device is connected.
Add to List	Click this button to add the LAN device information to the list below.
Share LAN resource List	
No.	The index number of share LAN device.
Active	Select or clear this check box to enable or disable the sharing of access to the LAN device.
Resource Name	This field displays the LAN device's name. Click the column heading to sort the entries by resource name.
IP Address	This field displays the IP address of the LAN device. Click the column heading to sort the entries by IP address.
MAC Address	This field displays the MAC address of the LAN device. Click the column heading to sort the entries by MAC address.
Interface	This field displays to which of the ZyAIR's interfaces the LAN device is connected. Click the column heading to sort the entries by interface.
Delete	Select a check box(es) and click **Apply** to delete the share device entry(es).
Delete All	Click this button to remove all of the share device entries.
Apply	Click **Apply** to save the changes.

Part IV:

Advanced Subscriber Account Management 2

This part covers the **ADVANCED PORTAL PAGE**, **ADVERTISEMENT**, **WALLED GARDEN**, **DDNS**, **LAN Devices**, **SYSLOG** and **WIRELESS** screens.

Chapter 14
Portal Page, Advertisement Links and Walled Garden

This chapter shows you how to set a portal web site, advertisement links and create walled garden web sites.

14.1 Portal Page Advertisement Links and Walled Garden Overview

When you enable subscriber authentication in the **Authentication Configuration** screen, you can set the ZyAIR to redirect a subscriber to a portal web site, display advertisement links or activate the walled garden feature for generating on-line advertising revenue.

14.2 Portal Page

A portal page is the first web site to which a subscriber is redirected after logging in successfully. The super user account also gets redirected to the portal page. Users are also redirected to this web site if you set up the ZyAIR to not require authentication or to require the acceptance of a user agreement before allowing Internet access. If you do not specify a portal web site, the subscriber will be directed to the intended web site specified.

Click **ADVANCED** and **PORTAL PAGE** to display the screen as shown next.

Figure 14-1PORTAL PAGE

The following table describes the labels in this screen.

Table 14-1PORTAL PAGE

LABEL	DESCRIPTION
URL Link	Enter the web site address of a portal page.
Apply	Click **Apply** to save the settings.

14.3 Advertisement Links

You can set the ZyAIR to display an advertisement web page as the first web page whenever the subscriber connects to the Internet. Click **ADVANCED** and **ADVERTISEMENT** to display the screen as shown next.

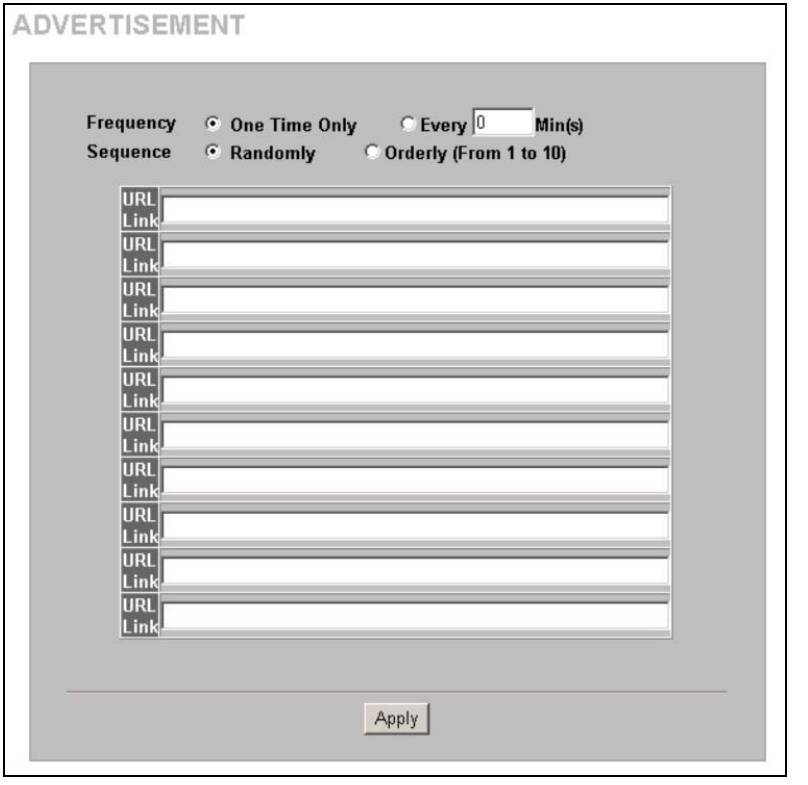


Figure 14-2 ADVERTISEMENT

The following table describes the labels in this screen.

Table 14-2 ADVERTISEMENT

LABEL	DESCRIPTION
Frequency	Select **One Time Only** to display an advertisement web site in an active browser window once after a subscriber logs in successfully. Select **Every … Min(s)** to display an advertisement web site in an active browser window once every time period specified (in minutes) after a subscriber logs in successfully. **The advertisement links are displayed randomly one at a time.**
URL Link	Enter the web site addresses in the fields provided.
Apply	Click **Apply** to save the changes.

14.4 Walled Garden

A subscriber must log in before the ZyAIR allows the subscriber access to the Internet. However, with a walled garden, you can define a web site address(es) which all subscribers can access without logging in.

Click **ADVANCED SETUP** and then **WALLED GARDEN** to display the screen as shown.

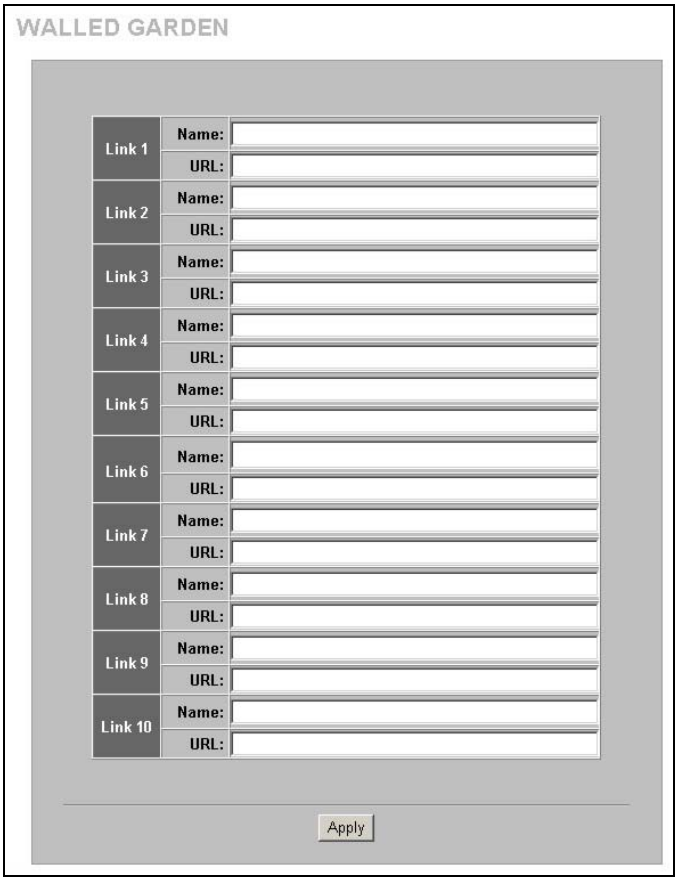


Figure 14-3 WALLED GARDEN

The following table describes the labels in this screen.

Table 14-3 WALLED GARDEN

LABEL	DESCRIPTION
Link 1 … 10	In the **Name** field, enter a descriptive name (up to 80 characters) for the walled garden link to be displayed in the web browser. In the **URL** field, enter the web site address (up to 200 characters) of the web site.
Apply	Click **Apply** to save the changes.

14.4.1 Walled Garden Login Example

The following figure shows the subscriber login screen with four walled garden links (the links are named **Walled Garden Link 1** through **4** for demonstration purposes, see *Table 14-3* to configure your own custom link names).

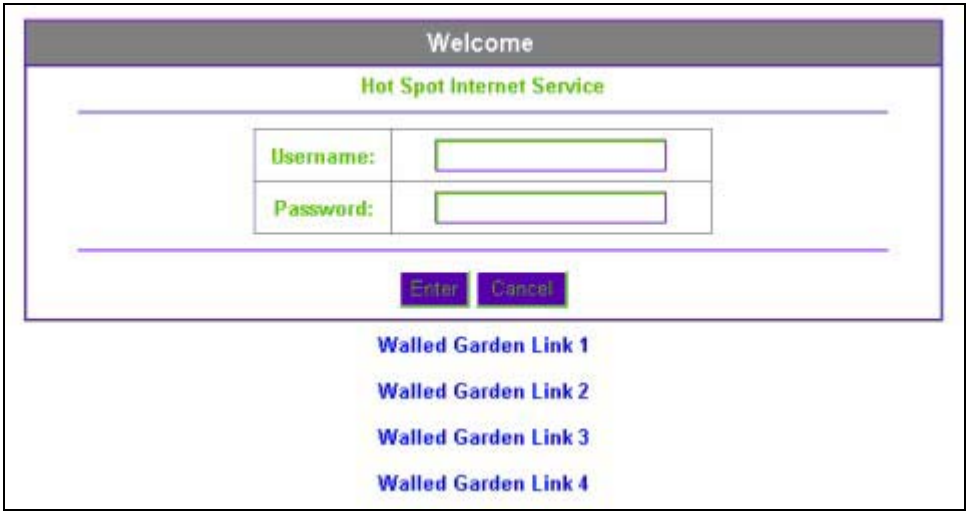


Figure 14-4 Walled Garden Login Example

Chapter 15
DDNS

This chapter shows you how to set the ZyAIR to use DDNS.

15.1 About DDNS

DDNS (Dynamic Domain Name System) allows you to update your dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe or other services). This is for cases where the ISP gives the ZyAIR a dynamic IP address but you still want to use a domain name. You can also access your FTP server or Web site on your own computer using a domain name (for example, myhost.dhs.org, where myhost is a name of your choice), which will never change instead of using an IP address that changes each time you reconnect.

You must go to the Dynamic DNS service provider's website and register a user account and a domain name before you can use the Dynamic DNS service with your ZyAIR.

The Dynamic DNS service provider will give you a password or key.

If you have a private WAN IP address, then you cannot use Dynamic DNS

15.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

15.2 Configuring DDNS

Click **ADVANCED** and **DDNS** to display the screen as shown next.

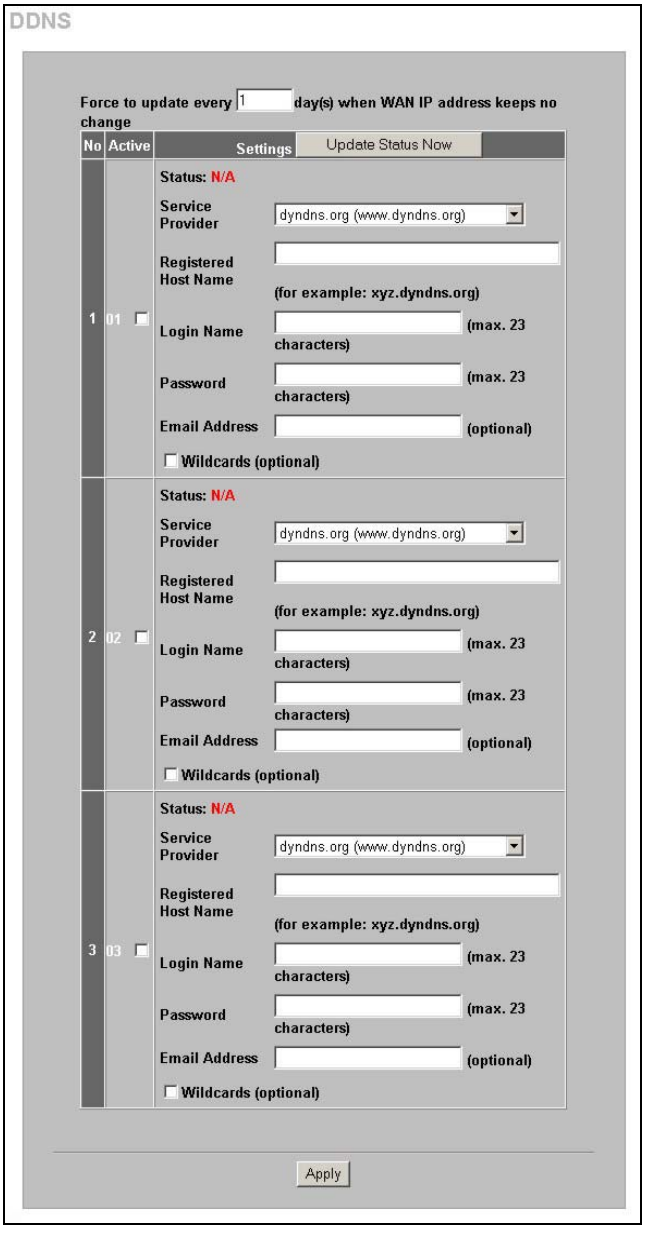


Figure 15-1 DDNS

The following table describes the labels in this screen.

Table 15-1 DDNS

LABEL	DESCRIPTION
Force to update every ~day(s) when WAN IP address keeps no change	Enter a number in the field to set the force update interval (in days). This sets how often the ZyAIR updates the DDNS server with the ZyAIR's WAN IP address when the ZyAIR's WAN IP address stays the same.
No	This is the index number of a DDNS account.
Active	Select or clear the check box to enable or disable the DDNS record.
Update Status Now	Click the **Update Status Now** button to have the ZyAIR update the DDNS server with the ZyAIR's WAN IP address.
Settings	Enter the DDNS server account information in the fields below.
Status	This field displays **N/A** when the DDNS client service is not installed. This field displays the time of the latest update (in YY/MM/DD HH:MM:SS format) and the current state of the DDNS Client. This field displays **Updated Successfully** when the DDNS client service is installed and running. This field displays **Update Fail** when the DDNS client service is installed, but the service is not running.
Service Provider	Select the name of your Dynamic DNS service provider.
Registered Host Name	Enter the host name in the field provided.
Login Name	Enter the user name for the above **Registered Host Name**. The Dynamic DNS service provider assigns you this user name.
Password	Enter the password for the above **Login Name**. The Dynamic DNS service provider assigns you this password.
Email Address	Enter your e-mail address. The DDNS server e-mails you important information once your Internet Name has been successfully registered.
Wildcards (optional)	Select the check box to enable DYNDNS Wildcard.
Apply	Click **Apply** to save the changes.

Chapter 16
LAN Devices

This chapter describes how you can remotely access devices on the LAN through the ZyAIR.

16.1 LAN Devices and NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

Traditionally, when you have a device (for example, a switch) on a LAN using NAT, you cannot access the device from the WAN since the LAN device is assigned a private IP address.

Your ZyAIR is a NAT-enabled device that makes your whole inside network appear as a single computer to the outside world.

16.1.1 Port Mapping

To make LAN devices behind the ZyAIR visible to the outside world, you configure a mapping between a virtual port on the ZyAIR and a server port on a LAN device. A virtual port is a port on the ZyAIR that appears as a physical port to the attached devices. A server port defines a server to which all specified requests are forwarded.

In addition, centralized LAN device management is possible through the ZyAIR using port mapping. You can access the management interface on the LAN device remotely provided that the LAN device has allowed remote management.

16.2 Configuring LAN Devices Port Mapping

Click **ADVANCED** and **LAN DEVICES** to display the screen as shown next.

You can configure port mapping for up to 50 LAN devices on the ZyAIR.

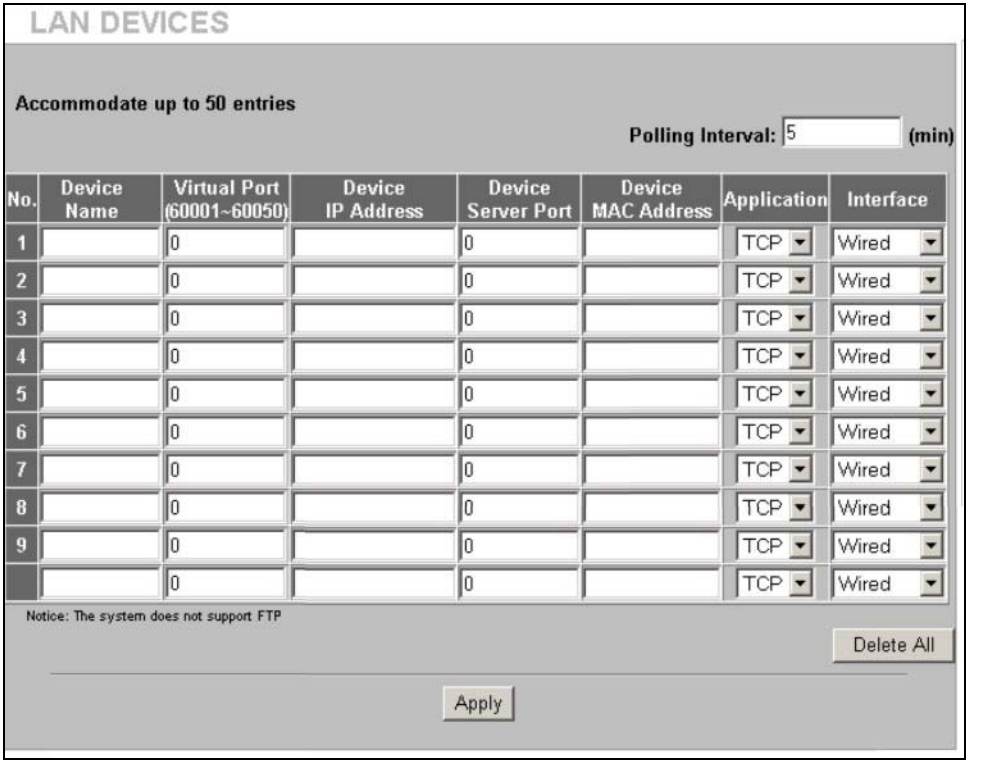


Figure 16-1 LAN DEVICES

The following table describes the labels in this screen.

Table 16-1 LAN DEVICES

LABEL	DESCRIPTION
Polling Interval	Specify the time interval (in minutes) between the ZyAIR's probes for device availability.
No.	This read-only field displays the index number of an entry.
Device Name	Enter the name (up to 20 characters) of the LAN device for identification purposes.
Virtual Port	Enter a unique port number between 60001 and 60050 to map to the port number in the **Server Port** field.

Table 16-1 LAN DEVICES

LABEL	DESCRIPTION
Device IP Address	Enter the IP address of a LAN device in dotted decimal notation. For example, 192.168.1.40.
Device Server Port	Enter the port number for a service (for example, 80 for HTTP) on the LAN device.
MAC Address	Enter the MAC address of the LAN device in hexadecimal notation in 6 hexadecimal pairs, for example, 0050BA8D2296. Make sure you enter the correct MAC address.
Application	Select an application type from the drop-down list box. Choose from **TCP** or **UDP**. Only requests for the selected application type are forwarded to the specified server port on the LAN device.
Interface	Select the ZyAIR's interface to which the LAN device is connected.
Delete All	Click **Delete All** to clear all entries. To delete a single entry, erase the contents in that entry.
Apply	Click **Apply** to save the changes.

16.2.1 LAN Device Management Example

In this example, there is a manageable switch and a wireless access point behind the ZyAIR and you want to be able to remotely access the web-based management interfaces on the manageable switch and access point over the Internet.

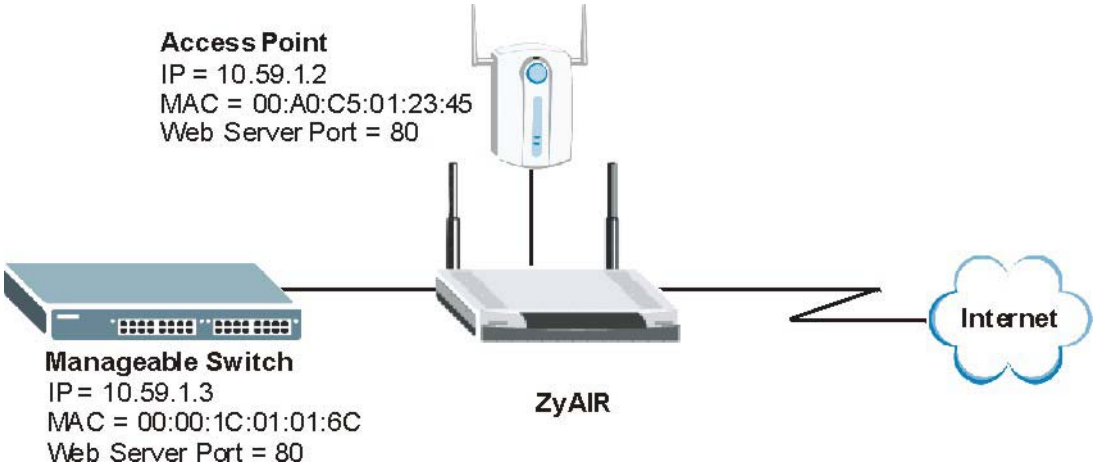


Figure 16-2 LAN Device Remote Management Example 1

You map virtual port 60001 on the ZyAIR to the web server port on the access point and 60002 to the web server port on the manageable switch.

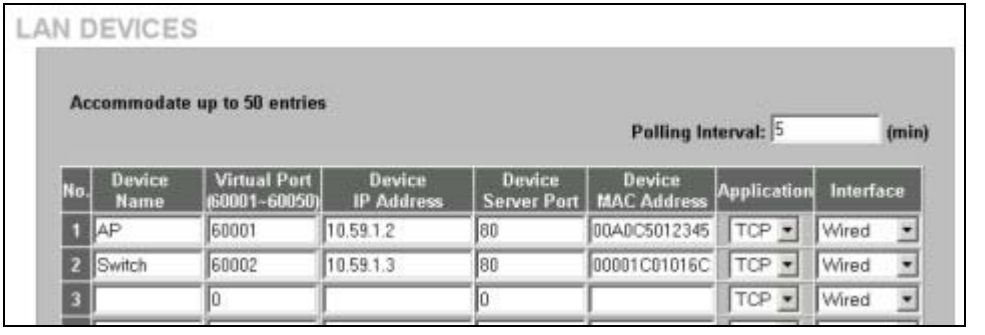


Figure 16-3 LAN Devices: Example 1

To access the web-based management interface, enter the WAN IP address of your ZyAIR and the virtual port number of the LAN device separated by a colon. In this example, to access the access point (AP), enter "http:// 192.168.1.1:60001" where 192.168.1.1 is the WAN IP address of the ZyAIR. The login screen of the LAN device management interface should display.

You can also access the LAN devices through the ZyAIR web configurator, refer to the section on accessing the LAN devices for more information.

16.2.2 Specifying an Inside Server Example

Let's say you have a web server behind the ZyAIR as shown in the next figure.

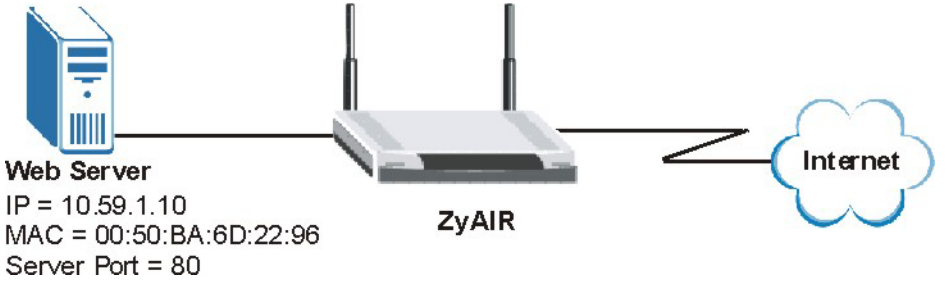


Figure 16-4 LAN Device Remote Management Example 2

In the **LAN Device Management** screen, you map virtual port 60001 to the server port (80) on the web server.

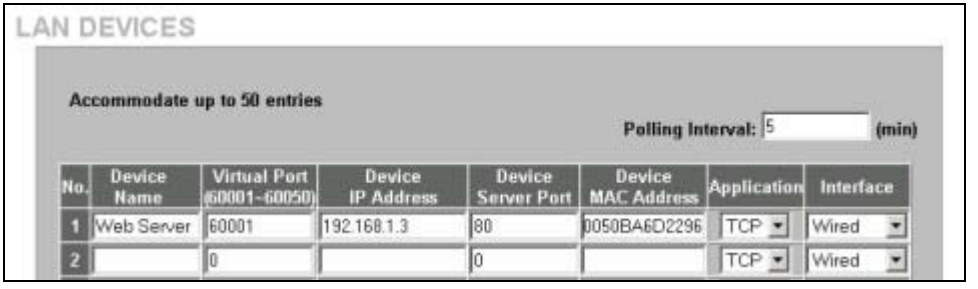


Figure 16-5 LAN Devices: Example 2

To access an inside server on the LAN, enter the WAN IP address of your ZyAIR and the virtual port number of the inside server separated by a colon. In this example, to access the web server, enter "http://192.168.1.1:60001" where 192.168.1.1 is the WAN IP address of the ZyAIR.

You can also access the server by entering the domain name provided that the ZyAIR has a domain name (or a dynamic domain name). Enter the domain name and the virtual port number separated by a colon, for example, http://www.domainName:60001.

You can also access the LAN devices through the ZyAIR web configurator, refer to the section on accessing the LAN devices for more information.

Chapter 17
Syslog

This chapter shows you how to configure syslog on the ZyAIR.

17.1 Syslog Configuration

Use the **SYSLOG Syslog** screen to configure to where the ZyAIR is to send logs.

To configure the syslog settings, click **ADVANCED**, **SYSLOG** to display the screen as shown next.

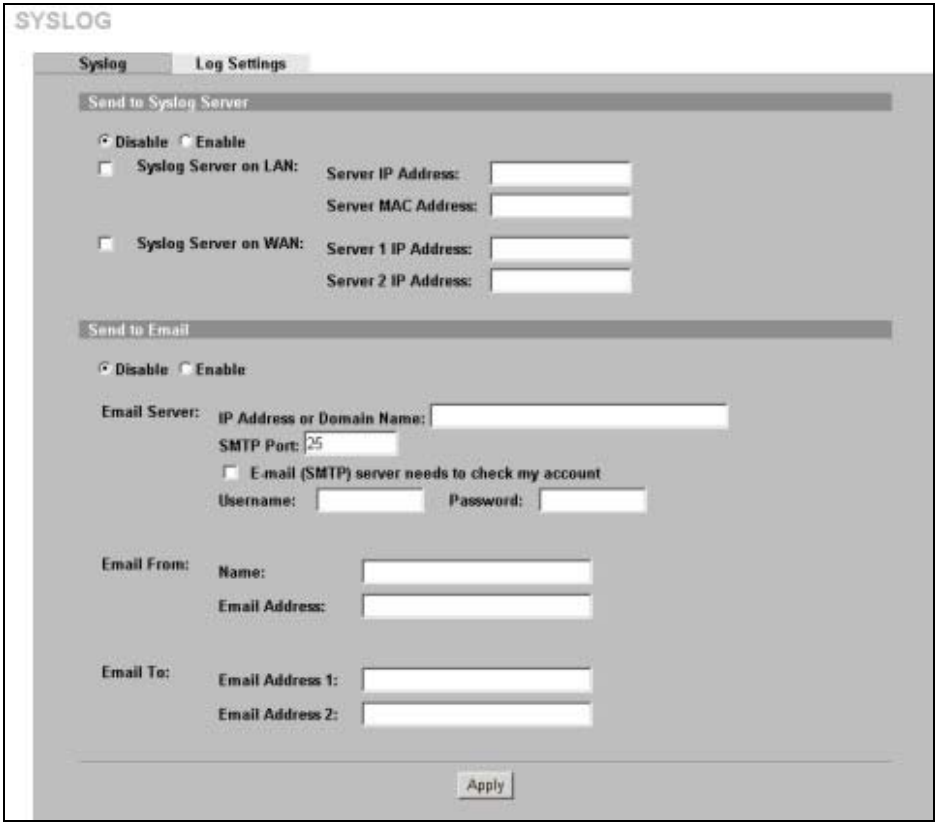


Figure 17-1 Syslog

The following table describes the labels in this screen.

Table 17-1 Syslog

LABEL	DESCRIPTION
Send to Syslog Server	Select **Enable** to activate the syslog function. Select **Disable** to de-activate the syslog function.
Syslog Server on LAN	Select this check box to specify a syslog server on the LAN.
Server IP Address	Enter the IP address (in dotted decimal notation) of the syslog server on the LAN.
Server MAC Address	Enter the MAC address of the syslog server on the LAN.
Syslog Server on WAN	Select this check box to specify a syslog server on the WAN.
Server 1 IP Address	Enter the IP address of the first syslog server on the WAN in dotted decimal notation.
Server 2 IP Address	Enter the IP address of the second syslog server on the WAN in dotted decimal notation.
Send to Email	Select **Enable** to have the ZyAIR send syslog messages to the e-mail account that you specify. Select **Disable** to not have the ZyAIR send syslog e-mail messages.
Email Server	
IP Address or Domain Name	Enter the IP address or domain name of the mail server for the e-mail addresses specified below. If this field is left blank, the syslog will not be sent via e-mail.
SMTP Port	Enter the port number (25, or between 2500 and 2599) for the mail server. The default is **25**.
E-mail (SMTP) server needs to check my account	Select this check box if your SMTP server requires user name and password authentication before accepting e-mail. Your network administrator, SMTP server provider or ISP should supply the username and password.
Username	Enter the username for the SMTP server.
Password	Enter the password for the SMTP server.
Email From:	
Name	Type a name that you want to be in the “message from” field of the log e-mail message that the ZyAIR sends.

Table 17-1 Syslog

LABEL	DESCRIPTION
Email Address	Enter your e-mail address. This is the address others use to send e-mail to **Email Address 1**/**Email Address 2**.
Email To:	
Email Address 1,2	Enter your first and second e-mail addresses to which the ZyAIR is to send the syslog e-mails. If you leave these fields blank, logs will not be sent via e-mail.
Apply	Click **Apply** to save the settings.

17.2 Syslog Log Settings Configuration

Use the **SYSLOG Log Settings** screen to configure which logs the ZyAIR is to send and the schedule for when the ZyAIR is to send the logs.

Click **ADVANCED**, **SYSLOG**, **Log Settings** to display the screen as shown next.

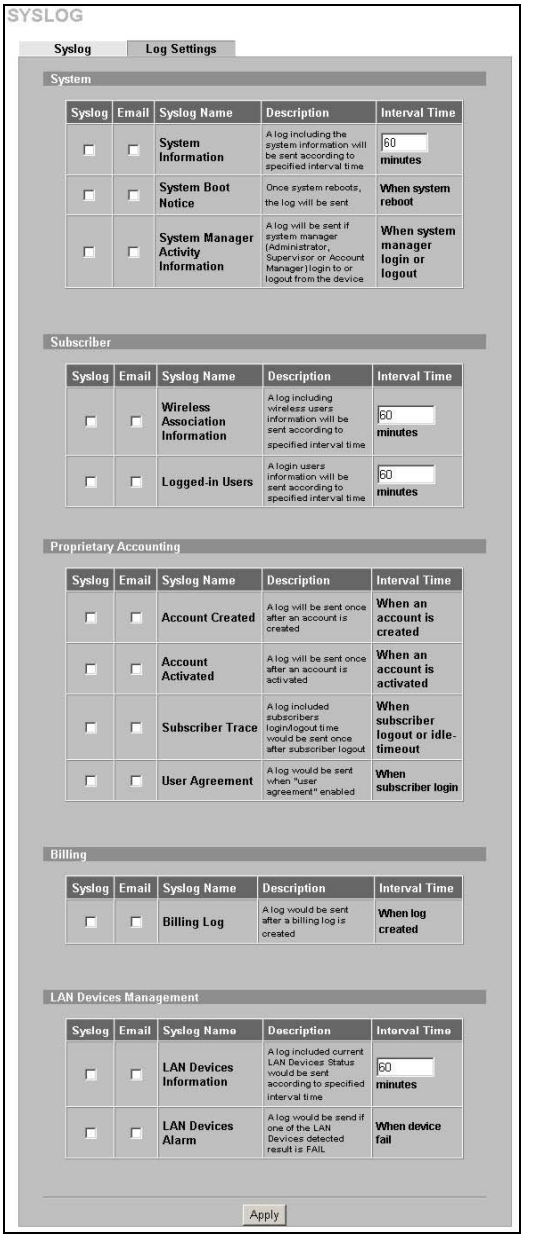


Figure 2 Log Settings

The following table describes the labels in this screen.

Table 17-2 Log Settings

LABEL	DESCRIPTION
Syslog	Select this check box to send this log information to your syslog server.
Email	Select this check box to send log information to the e-mail address specified in the **Syslog** screen**.**
Syslog Name	This field displays the name (or type) of the syslog. Select the check box(es) to send the syslog.
Description	This field displays a short description about the syslog.
Interval Time	This field displays how often the ZyAIR sends the syslog. If available, enter the number of minutes the ZyAIR waits between sending the syslog.
Apply	Click **Apply** to save the settings.

The following table describes the syslog formats.

Table 17-3 Log Formats

SYSLOG NAME	FORMAT	CREATED
System Information	**Id** <MAC Address> **System Uptime** <0 days 00h:04m:00s> **Location Name** <Location Name> **WAN** <FrameTxOK| FrameRxOK| FrameTxError| FrameRxError> **LAN** <FrameTxOK| FrameRxOK| FrameTxError| FrameRxError> **Wireless** <FrameTxOK| FrameRxOK| FrameTxError| FrameRxError>	Each time interval specified (between 1 and 10080 minutes).
System Boot Notice	**Id** <MAC Address> **System Up**	Each time when the device reboots.
System Manager Activity Information	**Id** <MAC Address> **System Account Activity Information** <Username, User IP, Status> Where: Username = Administrator | Supervisor | Accounting Operator User IP = IP Address Status = Login | Logout | Idle Time Out	Each time when a system manager logs in or logs out.

Table 17-3 Log Formats

SYSLOG NAME	FORMAT	CREATED
Wireless Association Information	**Id** <MAC Address> **Wireless Association Information** <Number of associated users, Start Number, End number) (Signal strength, Signal quality, Connection speed, MAC address>(…)(…)(…)	Each time interval specified (between 1 and 10080 minutes).
Logged-in Users	**Id** <MAC Address> **Logged-in Users** <Type, Number of logged-in users, Start Number, End number> Username, User IP, User MAC, Interface, Login time, RxData count, TxData count)(…)(…) Where: Type: Dynamic | Super | User agreement If the type of Logged-in user is Super Subscriber or User agreement, Username will be "********".	Each time interval specified (between 1 and 10080 minutes).
Account Created	**Id** <Mac Address> **Account Create** <Type, S/N, Username, Unit, Account usage time, Billing profile information> Where: Type: TimeToFinish | Accumulation | PostPaid Billing profile information = index, name Account usage time: 00:59:59 (example)	When an account is created.
Account Activated	**Id** <Mac Address> **Account Activate** < Username, User IP, User MAC, Interface >	When a subscriber account is activated.
Subscriber Trace	**Id** <MAC Address> **Subscriber Trace** <Type, Event, S/N, Username, User IP, User MAC, Interface, Login time, Logout time, Usage Time, Time Left, RxData count, TxData count) Where: Type: TimeToFinish | Accumulation | PostPaid | Super Event: Finished | Replenished | Logout | Idle-Timeout | Account Expired | Deleted If the type of Subscriber Trace is Super, the Username will be "********", and S/N will be "******". Usage time: 00:59:59 (example)	When a subscriber logs out.

Table 17-3 Log Formats

<table>
<tr><th>SYSLOG NAME</th><th>FORMAT</th><th>CREATED</th></tr>
<tr><td></td><td>Subscriber Trace Relationship
<table>
<tr><th>TYPE</th><th>EVENT</th><th>TIME LEFT</th></tr>
<tr><td>TimeToFinish</td><td>Finished</td><td>00:00:00</td></tr>
<tr><td>TimeToFinish</td><td>Replenished</td><td>00:12:00 to S/Nxxxxxx</td></tr>
<tr><td>TimeToFinish</td><td>Deleted</td><td>00:12:00</td></tr>
<tr><td>Accumulation</td><td>Finished</td><td>00:00:00</td></tr>
<tr><td>Accumulation</td><td>Replenished</td><td>00:12:00 to S/Nxxxxxx</td></tr>
<tr><td>Accumulation</td><td>Logout</td><td>00:48:00</td></tr>
<tr><td>Accumulation</td><td>Idle-Timeout</td><td>00:48:00</td></tr>
<tr><td>Accumulation</td><td>Deleted</td><td>00:48:00</td></tr>
<tr><td>Accumulation</td><td>Account Expired</td><td>00:48:00</td></tr>
<tr><td>PostPaid</td><td>Logout</td><td>******</td></tr>
<tr><td>PostPaid</td><td>Idle-Timeout</td><td>******</td></tr>
<tr><td>PostPaid</td><td>Deleted</td><td>******</td></tr>
<tr><td>PostPaid</td><td>Finished</td><td>******</td></tr>
<tr><td>PostPaid</td><td>Account Expired</td><td>******</td></tr>
<tr><td>Super</td><td>Idle-Timeout</td><td>******</td></tr>
<tr><td>Super</td><td>Deleted</td><td>******</td></tr>
</table></td><td></td></tr>
<tr><td>User Agreement</td><td>(Id, Mac Address) (User Agreement, Type, User IP, User MAC)
Where:
Type: Agree | Do not agree</td><td>When "user agreement" is enabled.</td></tr>
</table>

Table 17-3 Log Formats

SYSLOG NAME	FORMAT	CREATED
Billing Log	**Id** <Mac Address> **Billing Log** <, Type, S/N, Username, Billing profile information, Units, Usage time, Bill, Payment> Where: Type: TimeToFinish | Accumulation | PostPaid Billing profile name: [Name] Usage time: “00:59:59” (example) Billing profile information = index, name Payment: Cash | Credit Card “Credit Card” does not support “PostPaid”. If Type is “PostPaid”, the billing profile information and Units will be “*”.	When a billing log is created
LAN Devices Information	**Id** <MAC Address> **LAN Devices Information** <Number of devices, Start Number, End number> **Device name** <status> [additional information]	Each time interval specified (between 1 and 10080 minutes).
LAN Devices Alarm	**Id** <MAC Address> **LAN Device Alarm** <Device name, FAIL>	When the ZyAIR cannot connect to an attached LAN device.

Chapter 18
Wireless LAN

This chapter shows you how to configure wireless LAN settings on the ZyAIR and set up WEP encryption keys.

18.1 Wireless LAN Overview

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

18.1.1 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 and can set up an independent (wireless) network without the need of an access point (AP).

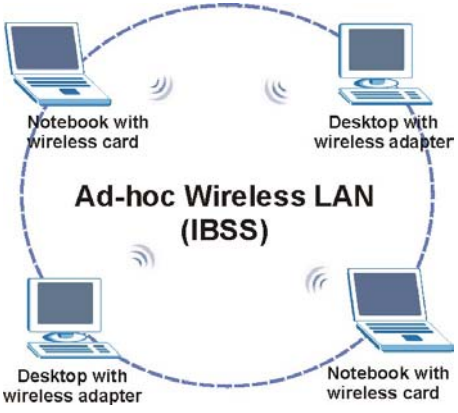


Figure 18-1 IBSS (Ad-hoc) Wireless LAN

18.1.2 BSS

A Basic Service Set (BSS) is 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.

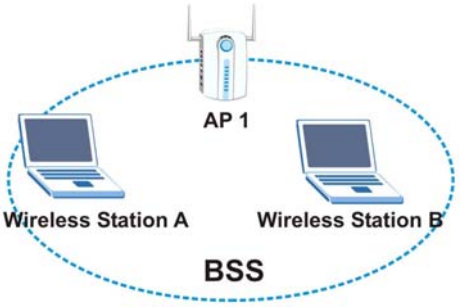


Figure 18-2 Basic Service set

18.1.3 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.

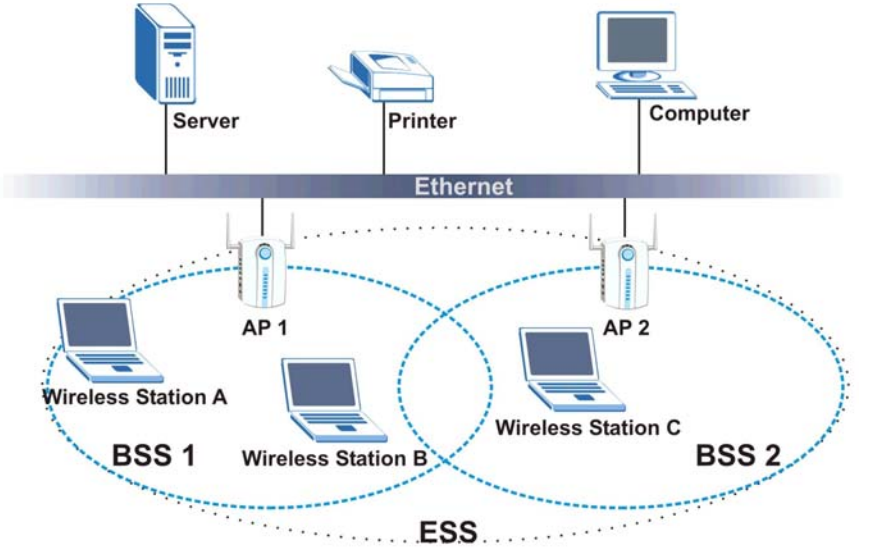


Figure 18-3 Extended Service Set

18.2 Wireless LAN Basics

This section provides background information on Wireless LAN features.

18.2.1 Channel

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

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

18.2.2 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. WEP degrades performance.

18.2.3 RTS/CTS

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

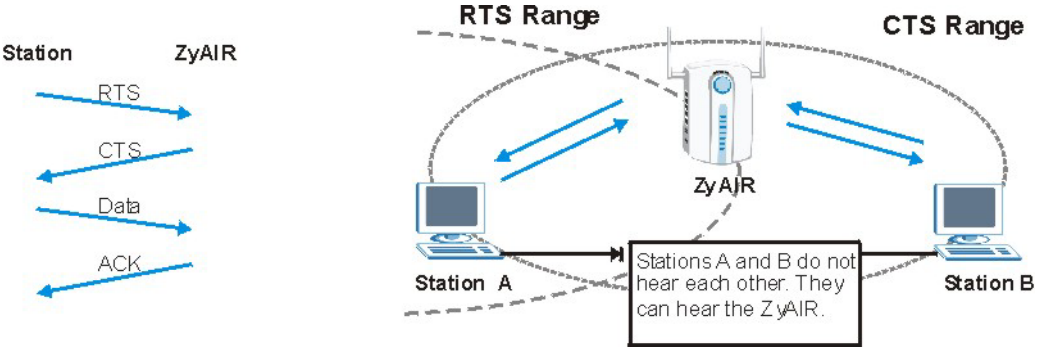


Figure 18-4 RTS/CTS

When station A sends data to the ZyAIR, it might not know that 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.

18.2.4 Fragmentation Threshold

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

18.2.5 Preamble Type

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

Long preamble mode allows more processing time for each transmitted data packet. Short preamble mode allows less processing time for the transmitted data packets.

Using short preamble mode may minimize overhead and maximize network throughput. However, short preamble mode is supported by IEEE 802.11b compliant wireless devices, thus wireless stations using short preamble mode cannot communicate with wireless stations using the original IEEE 802.11 standard.

18.3 Wireless LAN Setup

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.

Click **ADVANCED SETUP** and then **WIRELESS** to open the **Wireless** screen.

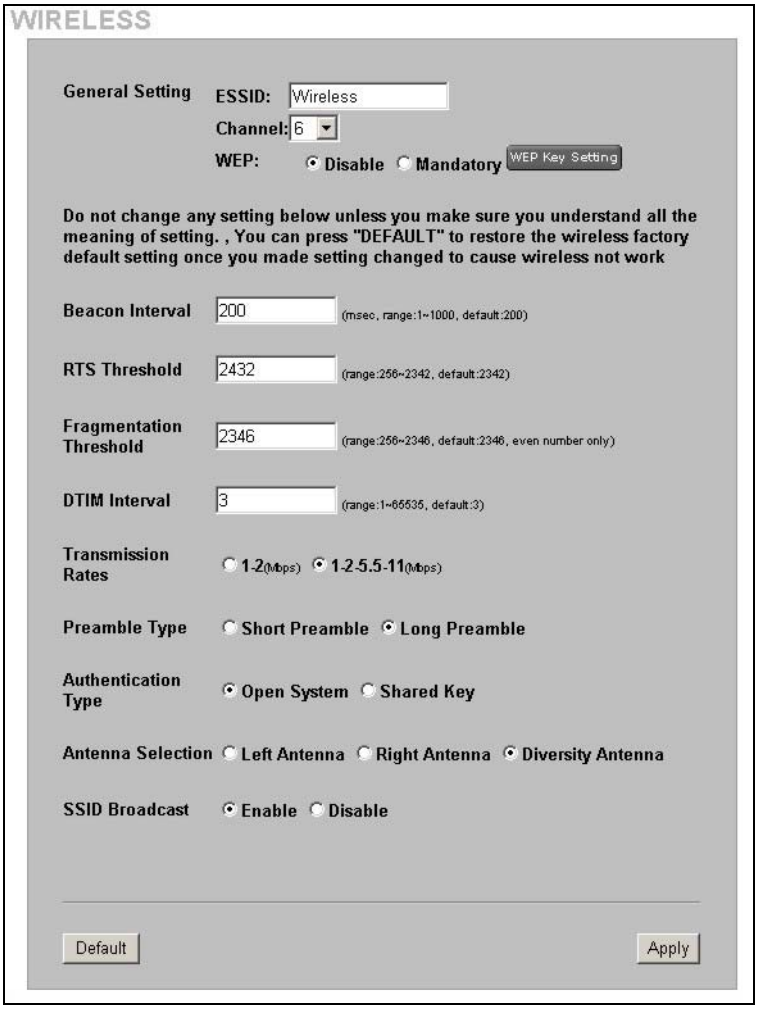


Figure 18-5 WIRELESS

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

Table 18-1 WIRELESS

LABEL	DESCRIPTION
ESSID	(Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. 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 click **Apply**. You must then change the wireless settings of your computer to match the ZyAIR's new settings.
Channel	Select a channel from the drop-down list box depending on your particular region.
WEP	Select **Disable** to allow all wireless computers to communicate with the access points without any data encryption. Select **Mandatory** to enable WEP data encryption. Then click **WEP Key Setup** to open a screen where you can configure the WEP keys on the ZyAIR. Refer to *Section 18.3.1*.
Beacon Interval	Set the number of milliseconds that should pass between sending out a beacon. Enter a time period between 1 and 1000. The default is **100**.
RTS Threshold	Enter a value between 0 and 2442 to enable an RTS/CTS handshake to avoid retransmitting due to hidden nodes. The default is **2432**.
Fragmentation Threshold	Enter a value between 256 and 2446 to enable a fragmentation threshold. This sets the maximum size of data fragments that can be sent. The default is **2432**. Use a low setting if there is a great deal of radio interference.
DTIM Interval	This setting, always a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells client devices that are set to power-save that a packet is waiting for them. The DTIM Interval's valid range is 1 to 65535.
Transmission Rates	The basic transfer rates should be set depending on the speed of your wireless network. The default setting is 1-2-5.5-11 (Mbps).
Preamble Type	Select either **Short Preamble** or **Long Preamble**.
Antenna Selection	Select **Left Antenna** if your device has removable antennas and you install a high-gain antenna on the connector on the left (when you look at the device's rear panel). Select **Right Antenna** if your device has removable antennas and you install a high-gain antenna on the connector on the right (when you look at the device's rear panel). Select **Diversity Antenna** (default) to have the device use the antenna that receives the best signal.

Table 18-1 WIRELESS

LABEL	DESCRIPTION
Authentication Type	Select **Open System** to allow any device to authenticate and then attempt to communicate with the ZyAIR. Using open authentication, any wireless device can authenticate with the ZyAIR, but the device can only communicate if its WEP keys match the ZyAIR. Devices not using WEP do not attempt to authenticate with a ZyAIR that is using WEP. Open authentication does not rely on a RADIUS server on your network. Select **Shared Key** to have the ZyAIR use shared key authentication. The ZyAIR sends an unencrypted challenge text string to any device attempting to communicate with the ZyAIR. The device-requesting authentication encrypts the challenge text and sends it back to the ZyAIR. If the challenge text is encrypted correctly, the ZyAIR allows the requesting device to authenticate. However, both the unencrypted challenge and the encrypted challenge can be monitored; thus leaving the ZyAIR open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network. Select **Both** to allow subscribers to communicate with or without data encryption.
SSID Broadcast	Select **Enable** to allow devices that do not specify an SSID (Service Set Identity) to associate with the ZyAIR. Select **Disable** to stop devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) from associating with the ZyAIR. The SSID on the subscriber's device must match the ZyAIR's SSID exactly.
Default	Click this button to load the factory default wireless LAN settings.
Apply	Click **Apply** to save the settings.

18.3.1 Configuring WEP Keys

When you select **Mandatory** in the **WEP Encryption** field in the **Wireless** screen, click **WEP Key Setting** to display the screen as shown.

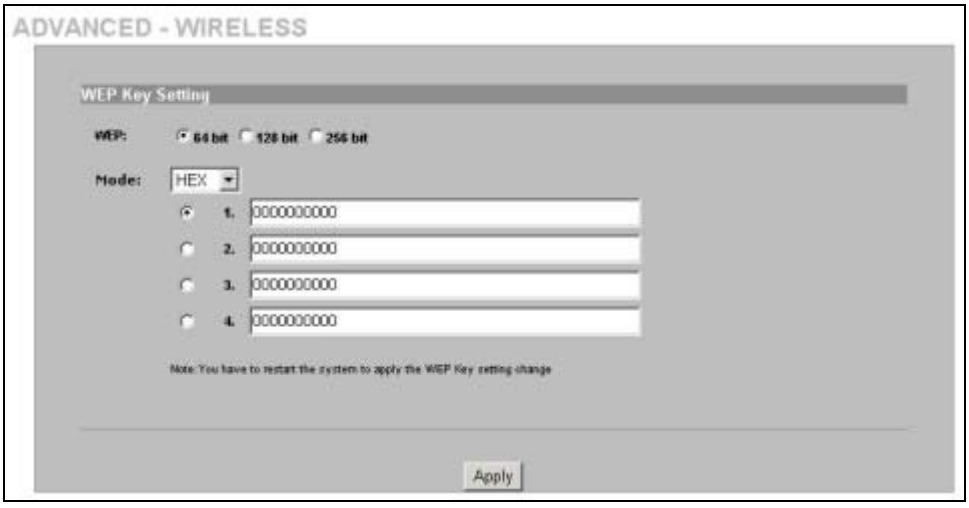


Figure 18-6 WEP Key Setup

The following table describes the labels in this screen.

Table 18-2 WEP Key Setup

LABEL	DESCRIPTION
WEP	Select **64 bit**, **128 bit** or **256 bit** for the WEP key length.
Mode	Select the type of input mode from the drop-down list box. Choices are **HEX** and **ASCII**. Select **ASCII** to enter the WEP keys as ASCII characters. Select **HEX** to enter the WEP keys as hexadecimal characters.

Table 18-2 WEP Key Setup

LABEL	DESCRIPTION
1 … 4	Enter the WEP keys in the fields provided and select a key as the default key to use. If you select **64 bit** in the **WEP Encryption** field. ◆ Enter either 10 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (e.g. 11AA22BB33) for HEX key type or ◆ Enter 5 printable ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (e.g. MyKey) for ASCII key type. If you select **128 bit** in the **WEP Encryption** field, ◆ Enter either 26 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 00112233445566778899AABBCC) for HEX key type or ◆ Enter 13 printable ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey12345678) for ASCII key type. If you select **256 bit** in the **WEP Encryption** field, ◆ Enter either 58 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” for HEX key type or ◆ Enter 29 printable ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” for ASCII key type. **ASCII WEP keys are case sensitive.**
Apply	Click **Apply** to save the changes.

Part V:

System Status, System Tools and Troubleshooting

This part covers the **SYSTEM STATUS** and **SYSTEM TOOLS** screens and troubleshooting.

Chapter 19
System Status

*This chapter describes the screens under **SYSTEM STATUS**.*

19.1 About System Status

The screens in **SYSTEM STATUS** show the current state of the ZyAIR.

19.2 View System Information

Click **SYSTEM STATUS** and **SYSTEM** to display the screen as shown next.

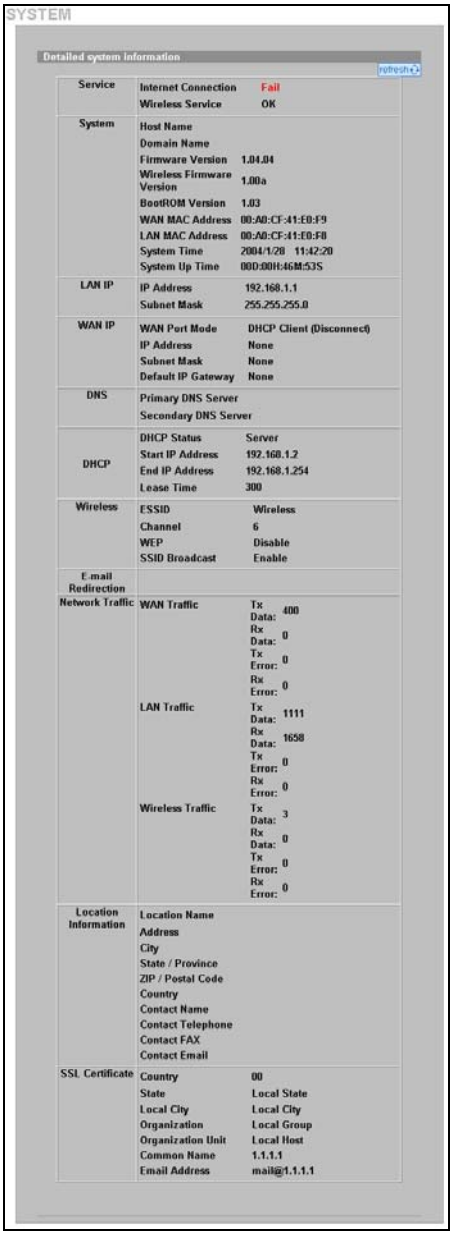


Figure 19-1 SYSTEM

The following table describes the labels in this screen.

Table 19-1 System

LABEL	DESCRIPTION
Service	
Internet Connection	This field displays the status of the ZyAIR's connection to the Internet.
Wireless Service	This field displays the status of the ZyAIR's wireless LAN.
System	
Host Name	This field displays the description name of the ZyAIR for identification purposes.
Domain Name	This field displays the domain name of the ZyAIR.
Firmware Version	This field displays the version of the firmware on the ZyAIR.
Wireless Firmware Version	This field displays the version of the wireless features on the ZyAIR.
Bootrom Version	This field displays the version of the bootbase in the ZyAIR.
WAN MAC Address	This field displays the MAC address of the ZyAIR on the WAN.
LAN MAC Address	This field displays the MAC address of the ZyAIR on the LAN.
System Time	This field displays the ZyAIR's current time.
System Up Time	This field displays the how long the ZyAIR has been operating since it was last started.
LAN IP	
IP Address	This field displays the IP address of the LAN port on the ZyAIR.
Subnet Mask	This field displays the subnet mask of the LAN port on the ZyAIR.
WAN IP	
WAN Port Mode	This field displays the DHCP mode of the WAN port. It displays **DHCP Client**, **Static IP Setting**, **PPPoE** or **PPTP**.
IP Address	This field displays the IP address of the WAN port on the ZyAIR.
Subnet Mask	This field displays the subnet mask of the WAN port on the ZyAIR.
Default IP Gateway	This field displays the IP address of the default gateway of the WAN port on the ZyAIR.
DNS	

Table 19-1 System

LABEL	DESCRIPTION
Primary DNS Server	This field displays the IP address of the primary DNS server.
Secondary DNS Server	This field displays the IP address of the secondary DNS server.
DHCP	
DHCP Status	This field displays the DHCP mode on the LAN.
Start IP Address	This field displays the first of the continuous addresses in the IP address pool.
End IP Address	This field displays the last of the continuous addresses in the IP address pool.
Lease Time	This field displays the time period (in minutes between 1 and 71582788) during which a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
Wireless	
ESSID	This field displays the ZyAIR's Extended Service Set IDentity.
Channel	This field displays the channel that the ZyAIR is using.
WEP	This field displays whether the ZyAIR is using WEP data encryption.
SSID Broadcast	This field displays whether the ZyAIR allows devices that do not specify an SSID (Service Set Identity) to associate with the ZyAIR. With "Enable", the ZyAIR allows devices that do not specify an SSID (Service Set Identity) to associate with the ZyAIR. With "Disable", the ZyAIR stops devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) from associating with the ZyAIR. The SSID on the subscriber's device must match the ZyAIR's SSID exactly.
E-mail Redirection	This field displays the IP address or the domain name of the SMTP server.
Network Traffic	
WAN Traffic	This field displays traffic statistics for the ZyAIR's WAN connection.
LAN Traffic	This field displays traffic statistics for the ZyAIR's LAN connection.
Wireless Traffic	This field displays traffic statistics for the ZyAIR's wireless LAN connection.
Location Information	
Location Name	This field displays the device's geographical location.

Table 19-1 System

LABEL	DESCRIPTION
Address	This field displays the street address of the device's location.
City	This field displays the city of the device's location.
State / Province	This field displays the state or province of the device's location.
ZIP/ Postal Code	This field displays the zip code or postal code for the device's location.
Country	This field displays the country of the device's location.
Contact Name	This field displays the name of the person responsible for this device.
Contact Telephone	This field displays the telephone number of the person responsible for this device.
Contact FAX	This field displays the fax number of the person responsible for this device.
Contact Email	This field displays the e-mail address of the person responsible for this device.
SSL Certificate	
Country	This field displays the two-letter abbreviation of your country.
State	This field displays the name of the state or province where your organization is located.
Local City	This field displays the name of the city your organization is located.
Organization	This field displays the name of your organization.
Origination Unit	This field displays additional information about your organization.
Common Name	This field displays the fully qualified domain name of your web server.
Email Address	This field displays your e-mail address.

19.3 Account List

Refer to the *Accounting* chapter for an example and explanation of the **ACCOUNT LIST** screen.

19.4 Account Log

The **ACCOUNT LOG** screen displays information on the ZyAIR's subscriber account logs.

Click **SYSTEM STATUS** and **ACCOUNT LOG** to display the screen as shown. Click a column heading to sort the entries if applicable.

Figure 19-2 ACCOUNT LOG

The following table describes the labels in this screen.

Table 2 ACCOUNT LOG

FIELD	DESCRIPTION
Clear Log	Click **Clear Log** to remove all of the log entries from the ZyAIR's memory and this screen.
Refresh	Click **Refresh** to update this screen.
SN	This field displays the index number of an entry. The maximum number of user account entries is 512.
Username	This field displays the account user name. Click the heading to sort the entries in ascending or descending order based on this column.
Time Created	This field displays when the account was created (in yyyy/mm/dd HH/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Login Time	This field displays when the subscriber logged in to use the account (in yyyy/mm/dd HH/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Usage Time	This field displays the amount of time the subscriber has purchased. Click the heading to sort the entries in ascending or descending order based on this column.

Table 2 ACCOUNT LOG

FIELD	DESCRIPTION
Charge	This field displays the total cost of the subscriber's account.
Payment Info	This field displays the subscriber's method of payment cash or credit.
Status	This field displays **IN-Used** when the account is currently in use. Otherwise it displays **UN-Used**. This field displays **Finished** when a subscriber uses up the time allocated to an account. This field displays **Expired** when a subscriber's account has reached expiration. This field displays **Replenished** and the serial number of the subscriber's account when a subscriber has purchased additional time units for the account.
Page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.

19.5 Current Users

The **CURRENT USER** screen displays a list of subscribers currently logged on to the ZyAIR for Internet access.

Click **SYSTEM STATUS** and **CURRENT USER** to display the screen as shown. Click a column heading to sort the entries if applicable.

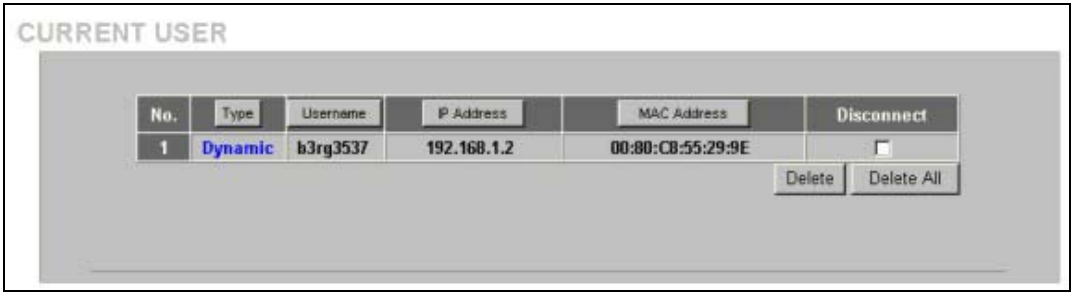


Figure 19-3 CURRENT USER

The following table describes the labels in this screen.

Table 19-3 CURRENT USER

LABEL	DESCRIPTION
No.	This field displays the index number of the entry.
Type	This field displays the type of account that the user has.
IP Address	This field displays the IP address of a subscriber's computer.
MAC Address	This field displays the MAC address of the computer that is logged in using the account.
Disconnect	Select this check box(es) and click **Delete** to terminate the selected subscriber connection.
Delete All	Click this button to terminate all subscriber connections.

19.6 DHCP Clients

The DHCP client table shows current DHCP client information of all network clients using the DHCP server on the ZyAIR.

Click **SYSTEM STATUS** and **DHCP** to display the screen as shown.

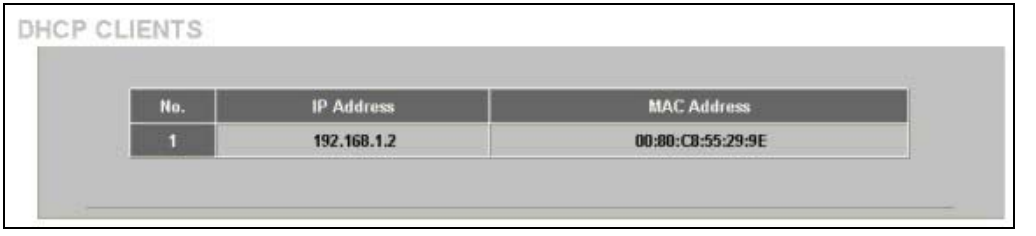


Figure 19-4 DHCP CLIENTS

The following table describes the labels in this screen.

Table 19-4 DHCP CLIENTS

LABEL	DESCRIPTION
No.	This field displays the index number of the entry.
IP Address	This field displays the IP address of the client computer.

Table 19-4 DHCP CLIENTS

LABEL	DESCRIPTION
MAC Address	This field displays the MAC address of the client computer. The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal characters). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address assigned to the client computer.

19.7 Session List

To display a list of incoming and outgoing packet information, click **SYSTEM STATUS** and **Session List**.

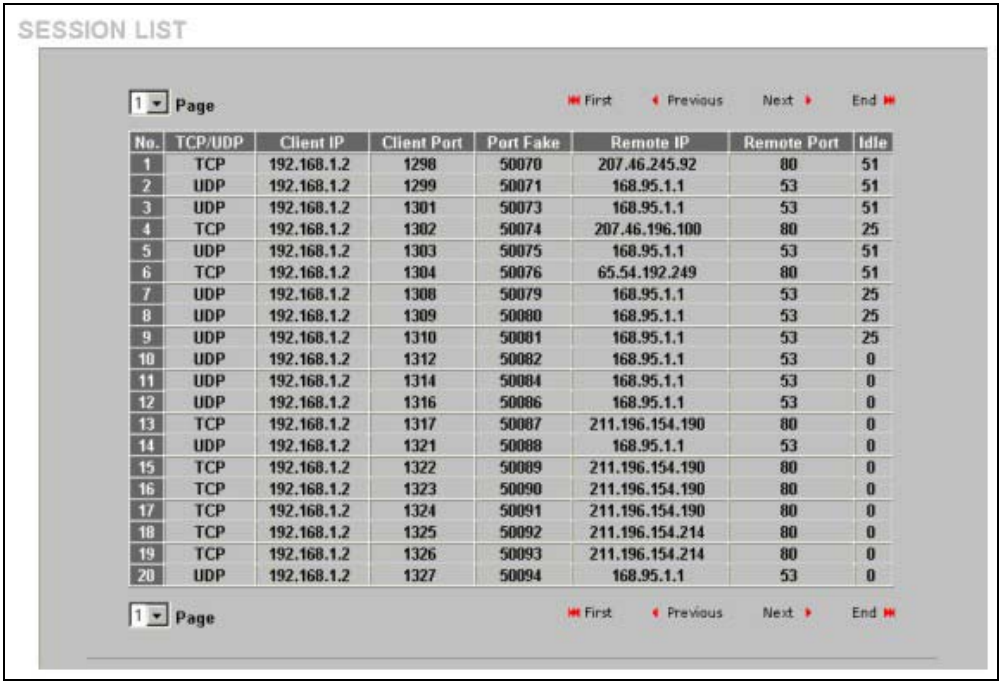


Figure 19-5 SESSION LIST

The following table describes the fields in this screen.

Table 19-5 SESSION LIST

LABEL	DESCRIPTION
Page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.
No	This field displays the index number of an entry.
TCP/UDP	This field displays the type of traffic (**TCP** or **UDP**).
IP Client	This field displays the IP address of the client computer.
Port Client	This field displays the port number through which the client computer transmits the traffic.
Port Fake	This field displays the NAT port to and from which the ZyAIR maps the session's traffic.
Remote IP	This field displays the IP address of a remote device the client computer accesses.
Remote Port	This field displays the port number of a remote device the client computer accesses.
Idle	This field displays how many seconds are left before the session times out if there is no more traffic. The ZyAIR automatically times out idle TCP sessions after 5 minutes (300 seconds). The ZyAIR automatically times out idle UDP sessions after 1 minute (60 seconds).

19.8 LAN Devices

The **SYSTEM STATUS LAN DEVICES** screen displays the status of LAN devices configured in the **ADVANCED LAN DEVICES** screen (refer to the *LAN Devices* chapter).

Click **SYSTEM STATUS** and **LAN DEVICES** to display the screen as shown next. This screen automatically updates every minute.

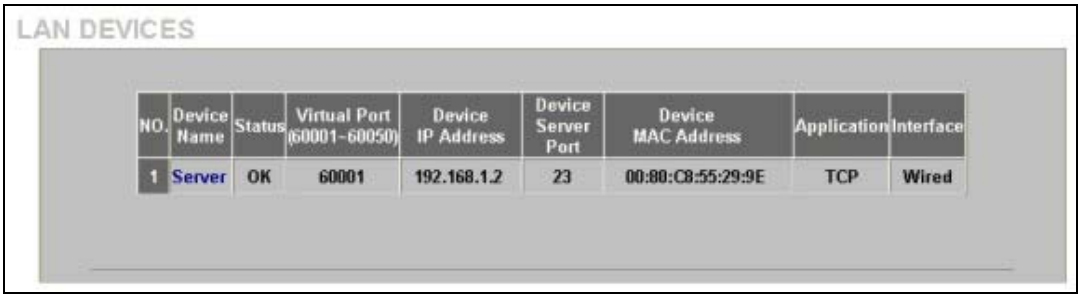


Figure 19-6 LAN DEVICES

The following table describes the labels in this screen.

Table 19-6 LAN DEVICES

LABEL	DESCRIPTION
No	This field displays the index number.
Device Name	This field displays the name of the LAN device. Click the device name to access the LAN device if the **Status** field is **OK**. For more information on accessing a LAN device, refer to *Section 19.8.1*.
Status	This field displays the current status of the LAN device. It displays **OK** when the LAN device is turned on and working properly. Otherwise it displays **Fail**.
Virtual Port (60001-60050)	This field displays the virtual port number.
Device IP Address	This field displays the IP address of the LAN device.
Device Server Port	This field displays the server port number of the LAN device.
Device MAC Address	This field displays the MAC address of the LAN device.
Application	This field displays the type of application packet that is forwarded to the LAN device.
Interface	This field displays to which interface on the ZyAIR the LAN device is connected.

19.8.1 Accessing a LAN Device

Before you can access a LAN device behind the ZyAIR, the following requirements must be met.

- The LAN device has a web-based management interface and it is enabled.

- You have set up the virtual port mapping to the LAN device server port in the **LAN Device Management** screen.
- The LAN device status is **OK** in the **LAN Device Status** screen.

There are two methods to access the LAN device: directly or through the web configurator.

To access the LAN device through the web configurator, open the **LAN Device Status** screen and click the device name. A new Internet browser should display showing the login screen of the LAN device management interface.

To directly access the LAN device, enter the WAN IP address of your ZyAIR and the virtual port number of the LAN device separated by a colon. For example, enter “http:// 192.168.1.1:60001” where 192.168.1.1 is the WAN IP address of the ZyAIR. The login screen of the LAN device management interface should display.

Chapter 20
Configuration, Firmware and Accounting Log Maintenance

This chapter shows you how to upgrade the firmware and configuration file and back up configuration files and accounting logs.

20.1 Filename Conventions

The configuration file contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. Once you have customized the settings of the ZyAIR, they can be saved back to your computer under a filename of your choosing.

It is recommended to use the ".bin" file extension for the firmware file and ".rom" for the configuration file for management purposes.

Visit www.zyxel.com to download the latest version of firmware for your ZyAIR.

20.2 Configuration File Maintenance

You can use the web configurator to perform configuration file backup and restore. Backing up the configuration allows you to back up (save) the device's current configuration to a file. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR DEVICE.

20.2.1 Backup Configuration Using HTTP

Use the following procedure to use HTTP to back up the device's current configuration to a file on your computer.

Step 1. Click **SYSTEM TOOLS** and **CONFIGURATION**. A screen displays as shown next.

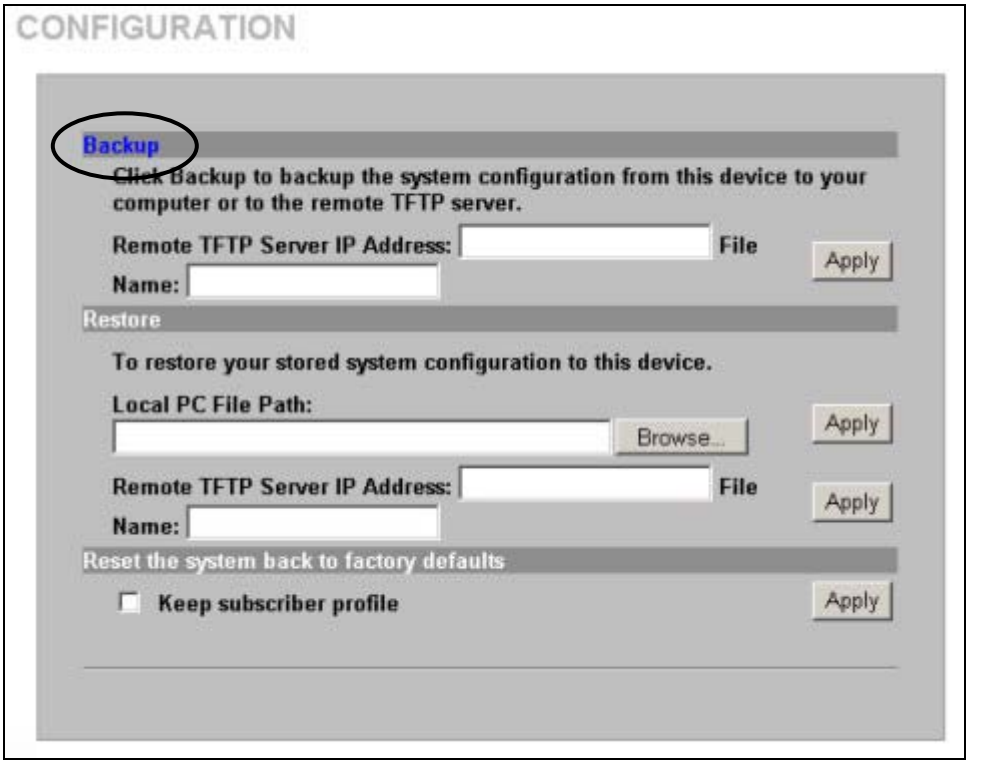


Figure 20-1 CONFIGURATION: Backup Using HTTP

Step 2. Click **Backup**. A **File Download** window displays as shown next.

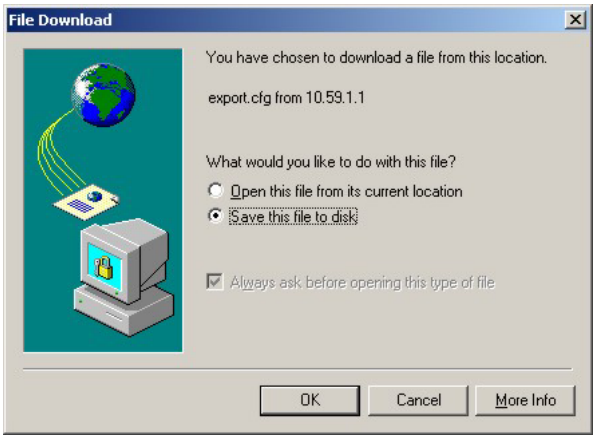


Figure 2 Configuration Backup: File Download

Step 3. Select **Save this file to disk** and click **OK**. A **Save As** window displays.

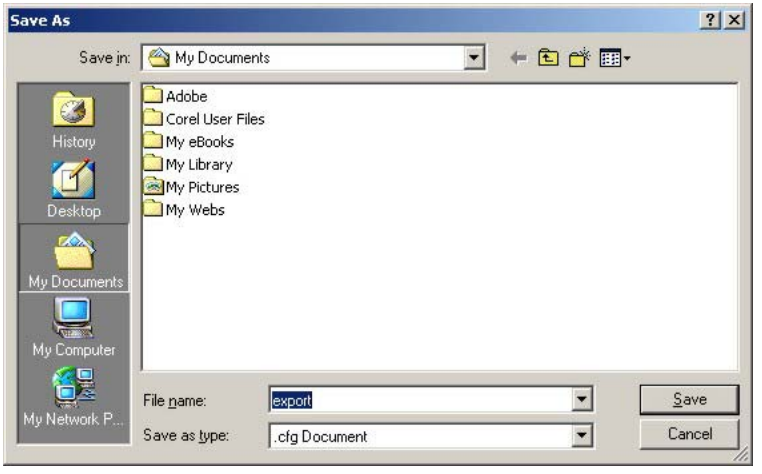


Figure 20-3 Configuration Backup: Save As

Step 4. Specify the file name and/or location and click **Save** to start the backup process.

20.2.2 Backup Configuration Using TFTP

Use the following procedure to use TFTP to back up the device's current configuration to a file on a TFTP server.

Step 1. Click **SYSTEM TOOLS** and **CONFIGURATION**. A screen displays as shown next.

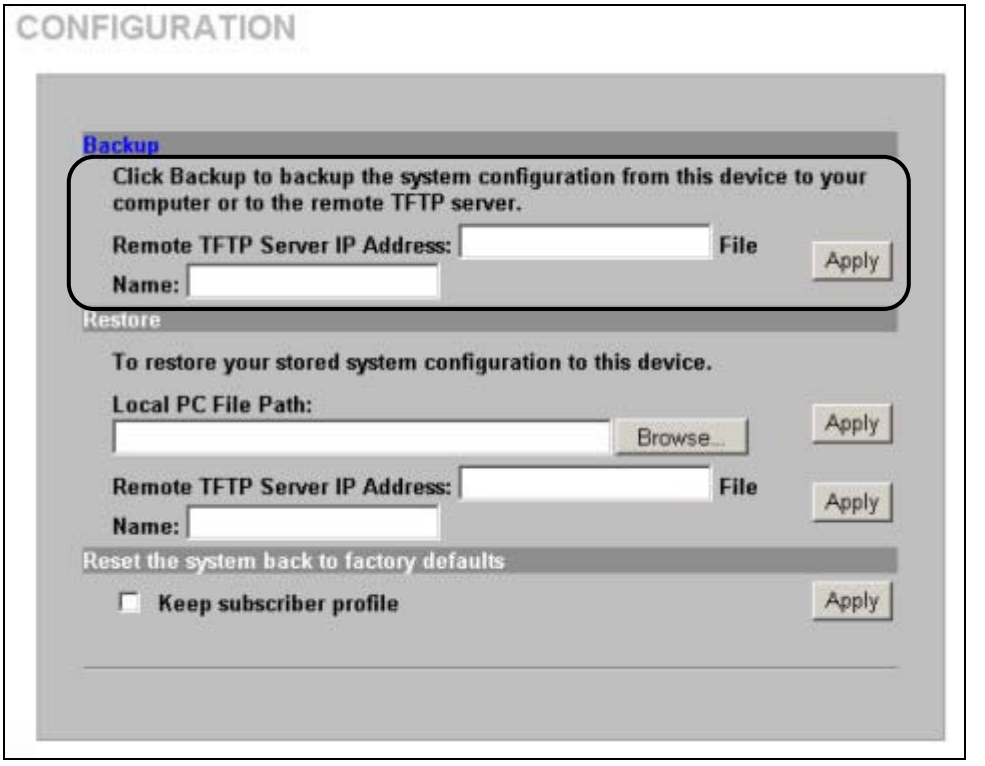


Figure 20-4 CONFIGURATION: Backup using TFTP

Step 2. Enter the IP address of the TFTP server in dotted decimal notation in the **Remote TFTP Server IP Address** field.

Step 3. Specify a file name for the configuration backup in the **File Name** field.

Step 4. Click **Apply**. When the file transfer process is complete, a screen displays as follows.

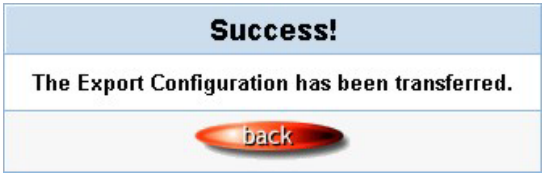


Figure 20-5 Configuration Backup: Using TFTP Successful

20.2.3 Restore Configuration Using HTTP

This section shows you how to upload a new or previously saved configuration file from your computer to your ZyAIR.

This function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

Step 1. Click **SYSTEM TOOLS** and **CONFIGURATION**. A screen displays as shown next.

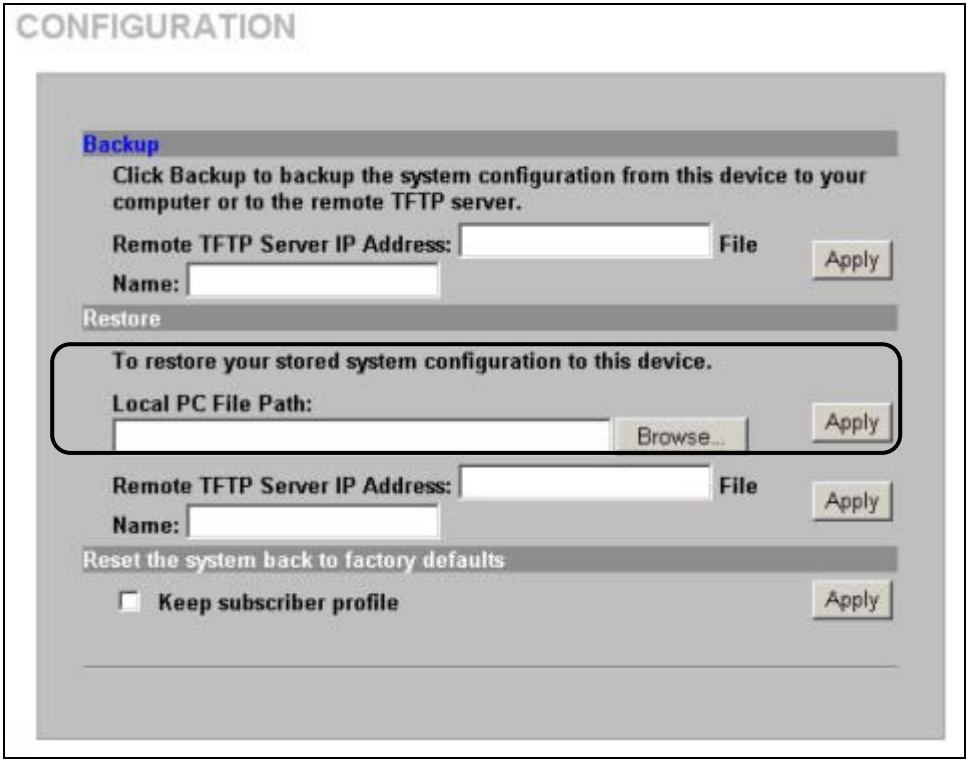


Figure 20-6 CONFIGURATION: Restore Using HTTP

Step 2. Specify the location and filename of a configuration file in the **Local PC File Path** field or click **Browse**.

Step 3. Click **Apply** to start the configuration restore process. The ZyAIR automatically restarts after the restoration process is complete.

20.2.4 Restore Configuration Using TFTP

This section shows you how to upload a new or previously saved configuration file from a TFTP server to your ZyAIR.

This function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

Step 1. Click **System Tools** and **Configuration**. A screen displays as shown next.

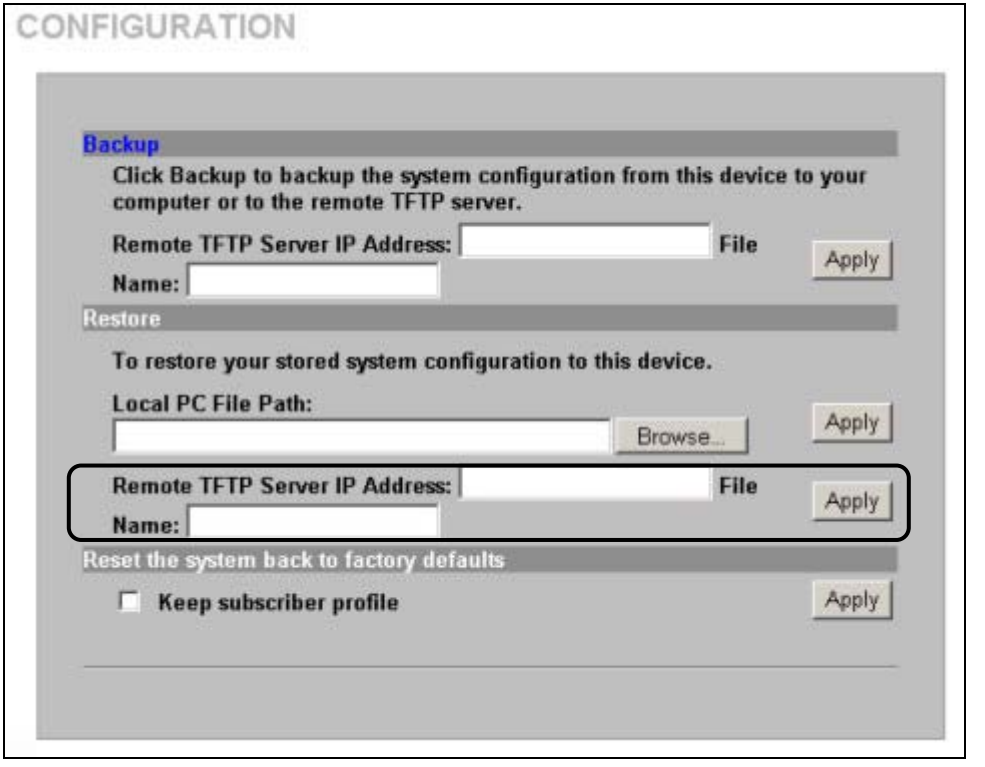


Figure 20-7 CONFIGURATION: Restore Using TFTP

Step 2. Enter the IP address of the TFTP server in dotted decimal notation in the **Remote TFTP Server IP Address** field.

Step 3. Specify a file name for the configuration backup in the **File Name** field.

Click **Apply** to start the configuration restore process. The ZyAIR automatically restarts after the restoration process is complete.

20.3 Firmware Upgrade

There are two ways to upgrade firmware to the ZyAIR: manually or scheduled.

To manually upgrade the firmware, you have to download the latest firmware first from www.zyxel.com and then upload it to the ZyAIR.

With scheduled firmware upgraded, you need to set up a TFTP server where the ZyAIR can automatically download the latest firmware at the specified time.

20.3.1 Manual Firmware Upgrade Using the Web Configurator

Follow the steps below to upload the firmware using the web configurator.

Step 1. Click **SYSTEM TOOLS**, **FIRMWARE** and then **Manual Firmware Upgrade** to display the screen as shown.

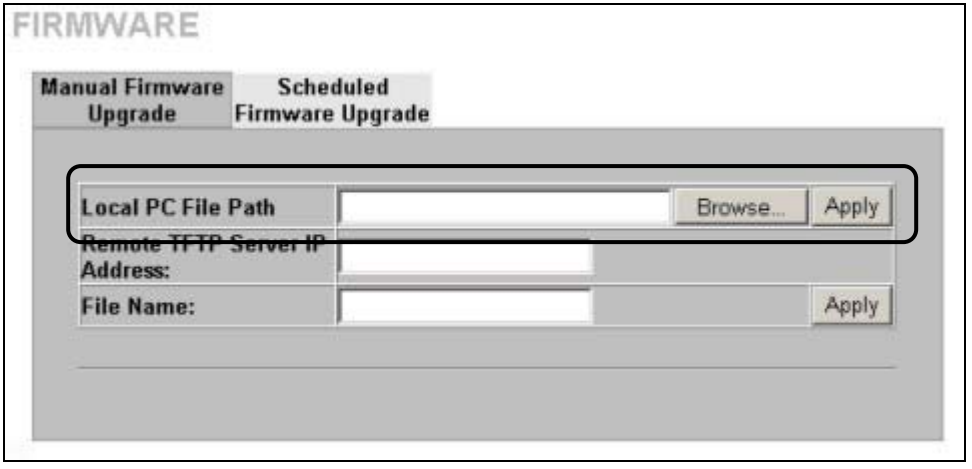


Figure 20-8 Manual Firmware Upgrade Using the Web Configurator

Step 2. Specify the name of the firmware file in the **Local PC File Path** field or click **Browse** to locate the file and click **Apply** to start the file transfer process. The firmware must be a binary file and should have a .bin extension.

Step 3. When the file transfer is completed successfully, a restart message displays and the ZyAIR automatically restarts.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

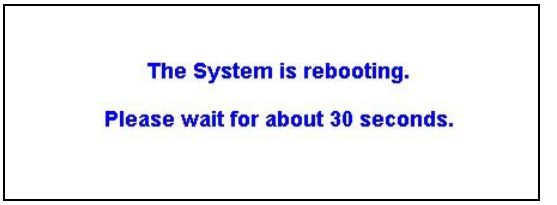


Figure 20-9 System Restart

Step 4. After the ZyAIR finishes restarting, access the web configurator again. Check the firmware version number in the **System** screen.

When the ZyAIR restarts, all connections terminate. Subscribers need to log in again.

20.3.2 Manual Firmware Upgrade via TFTP Server

Follow the steps below to upload the firmware using the web configurator.

Step 1. Download the latest firmware from www.zyxel.com and store it in a TFTP server. Unzip the file if it is zipped.

Step 2. Run a TFTP server program and specify the location of the firmware file and the communication mode. Refer to the documentation that comes with your TFTP server program for instructions.

Step 3. Access the web configurator. Refer to the section on accessing the web configurator for instructions.

Step 4. Click **SYSTEM TOOLS**, **FIRMWARE** and then **Manual Firmware Upgrade** to display the screen as shown.

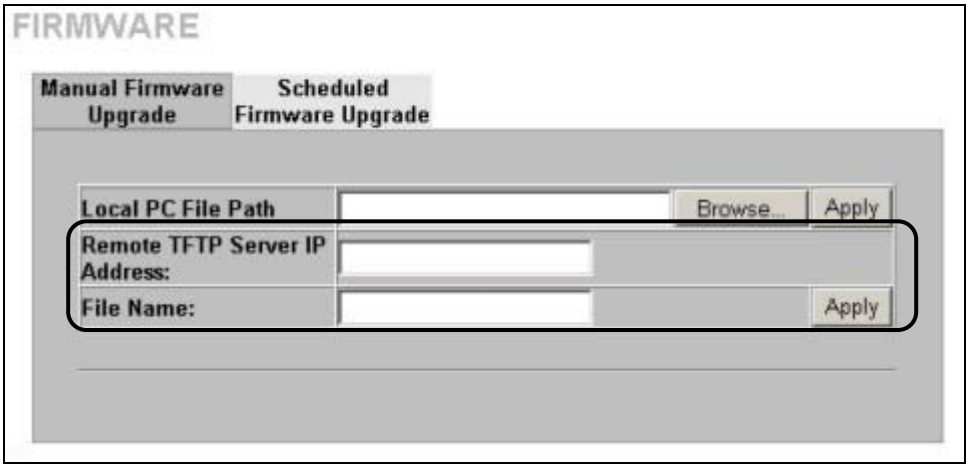


Figure 10 Manual Firmware Upgrade via TFTP Server

Step 5. Specify the IP address of the TFTP server in the **TFTP Server IP Address** field.

Step 6. Specify the name of the firmware file in the **File Name** field.

Step 7. Click **Apply** to start the file transfer process.

Step 8. When the file transfer is completed successfully, the following message displays and the ZyAIR automatically restarts to complete the firmware upgrade process.

Step 9. After the ZyAIR finishes restarting, access the web configurator again. Check the firmware version number in the **System Status** screen.

20.3.3 Scheduled Firmware Upgrade

Click **SYSTEM TOOLS**, **FIRMWARE** and then **Scheduled Firmware Upgrade** to display the screen as shown.

Configure the screen to automatically download the latest firmware from a TFTP server.

Make sure that the TFTP server has the firmware and synchronization check file before you configure for scheduled firmware upgrades.

Make sure that you check new features or functionality enhancements in new firmware releases before you put the firmware on the TFTP server.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

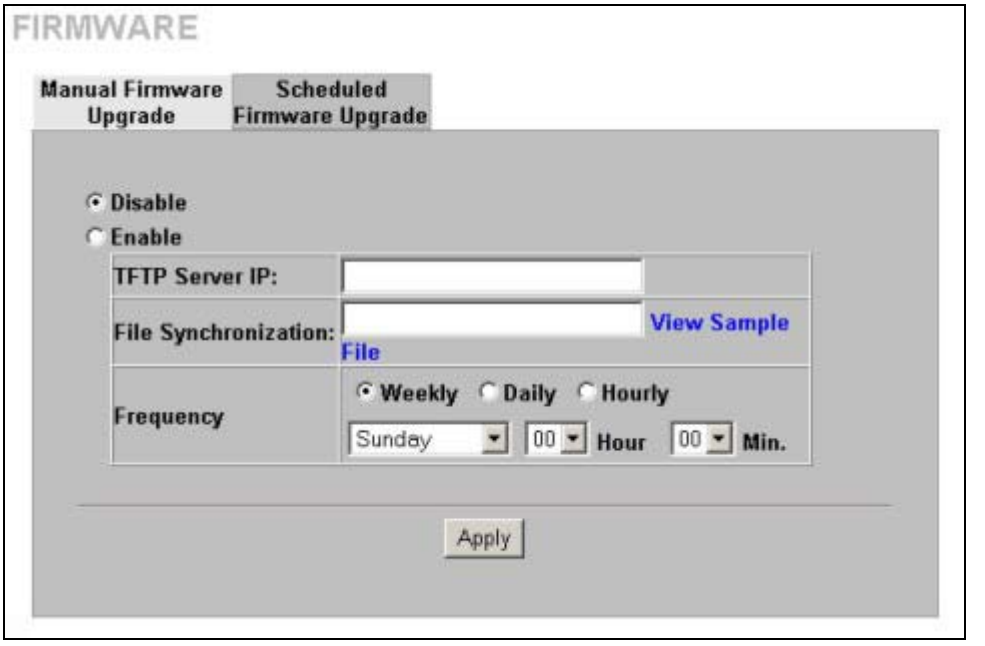


Figure 20-11 Scheduled Firmware Upgrade

When the ZyAIR restarts, all connections terminate. Subscribers need to log in again.

Table 20-1 Scheduled Firmware Upgrade

LABEL	DESCRIPTION
Disable Enable	Select **Disable** or **Enable** to turn the scheduled firmware upgrade function on or off (disabled by default).
TFTP Server IP	Type the IP address of the TFTP server from which the ZyAIR can download new firmware files.
File Synchronization	A synchronization check file is a .txt file containing the latest firmware filename and version number on the TFTP server. Enter the name of the check file.
View Sample File	Click **View Sample File** to view an example synchronization check file (see *Figure 20-12*).

Table 20-1 Scheduled Firmware Upgrade

LABEL	DESCRIPTION
Frequency	Set how often (**Weekly**, **Daily** or **Hourly**) you want to have the ZyAIR check for new firmware and upgrade to new firmware if available (default **Weekly**). Then select the day (applies only when you select **Weekly**), the hour (applies when you select **Daily** or **Hourly**) and the minute that you want the ZyAIR to do the check and upload.
Apply	Click **Apply** to save the changes.

The following figure shows an example of a check file's content.

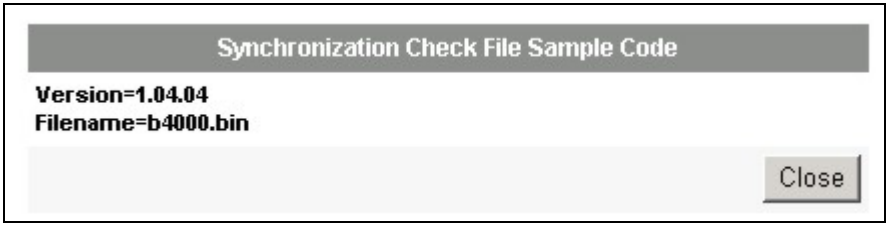


Figure 20-12 Synchronization Check File Example

Chapter 21
SSL (Secure Socket Layer) Security

This chapter shows you how to setup and enable Secure Socket Layer (SSL) security on the ZyAIR.

21.1 About SSL

SSL (Secure Socket Layer) security is a standard Internet protocol for secure communications that uses a combination of certificate-based authentication and public-key encryption. SSL protects data transfer between the web configurator on the ZyAIR and the web browser on a connected computer.

With SSL security activated, data (such as user name and password) transferred between the ZyAIR and the computer is protected when you access the ZyAIR using a web browser that supports SSL.

21.2 Activating SSL Security for Management Connections

Follow the steps below to activate the SSL security for management connections to the ZyAIR.

Step 1. Click **ADVANCED** and then **SERVER**. Select the **SSL Security** check box under **Web Server**.

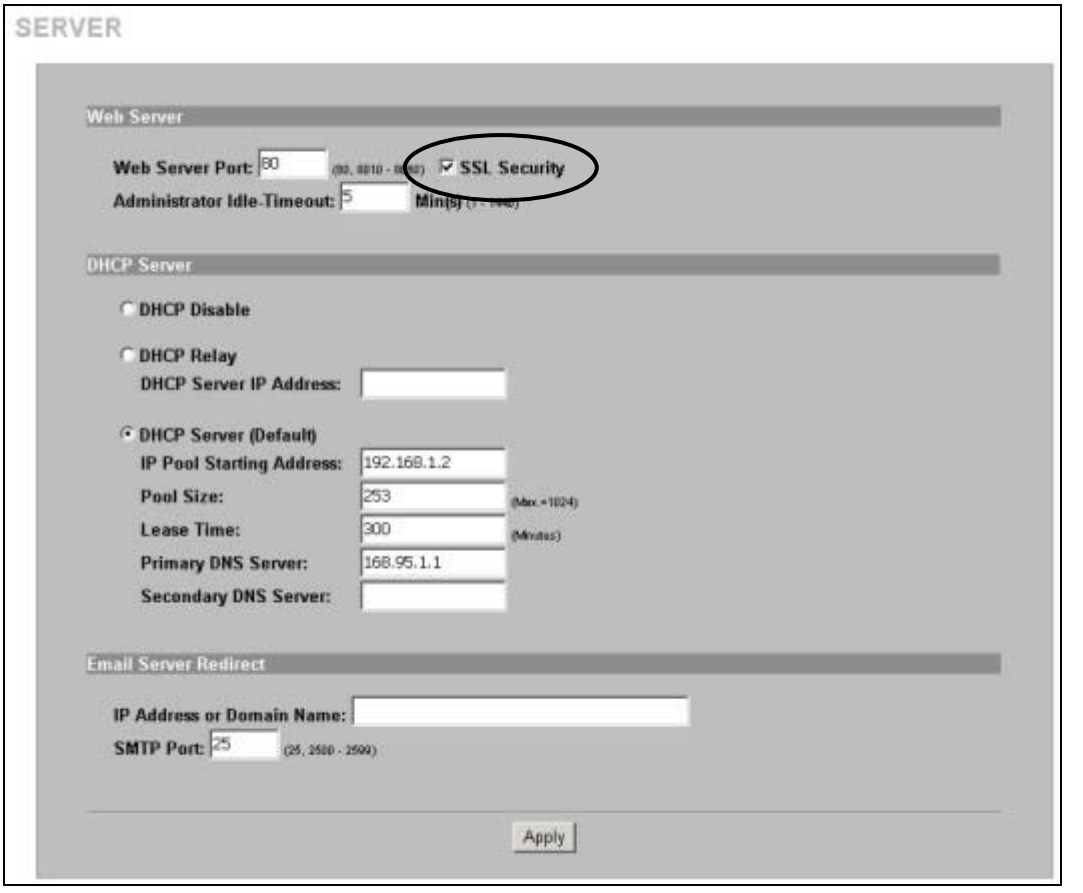


Figure 21-1 System Settings: Server Configuration: Enable SSL Security

Step 2. Click **Apply** to save the changes and restart the ZyAIR when prompted. See section *21.3* for details on how to install the SSL security certificate in order to access the web configurator through a secure connection.

21.3 Viewing and Installing the SSL Security Certificate

After you enable and activate the SSL security on the ZyAIR, you can access the web configurator through a secure connection.

Follow the steps below to view and install the default SSL security certificate on your computer.

Step 1. Access the ZyAIR. A **Security Alert** window displays. Click **OK** to continue and close the window.

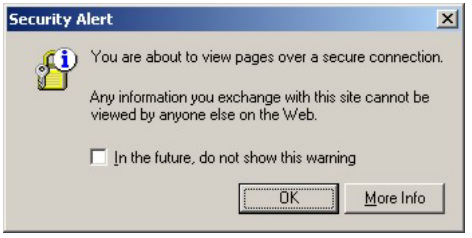


Figure 21-2 Installing the SSL Security Certificate: First Security Alert

Step 2. A second **Security Alert** window displays.

Figure 21-3 Installing the SSL Security Certificate: Second Security Alert

Step 3. Click **View Certificate** to display the **Certificate** window as shown.

Figure 21-4 Installing the SSL Security Certificate: View Certificate

Step 4. Click **Install Certificate** to install the certificate to your computer. A **Certificate Import Wizard** window displays. Click **Next**.

Figure 21-5 Installing the SSL Security Certificate: Certificate Import Wizard

Step 5. Accept the default or specify the location to store the certificate. Click **Next**.

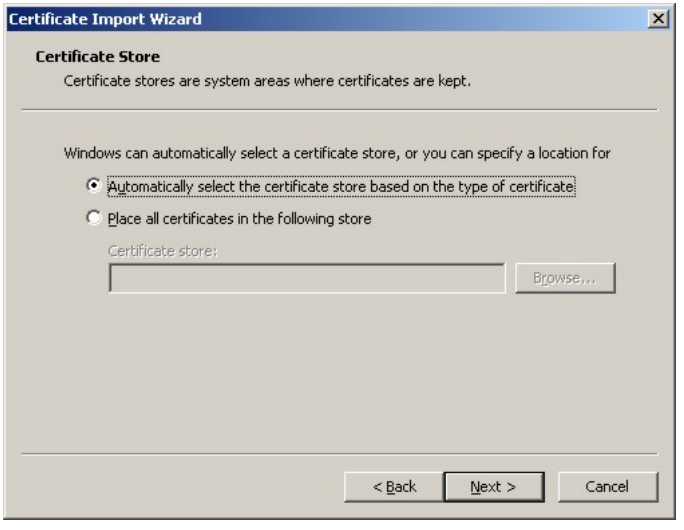


Figure 21-6 Certificate Import Wizard: Location

Step 6. Click **Finish** to import the certificate.

Figure 21-7 Certificate Import Wizard: Finish

Step 7. A **Root Certificate Store** window displays as shown. Click **Yes** to store the certificate to the computer.

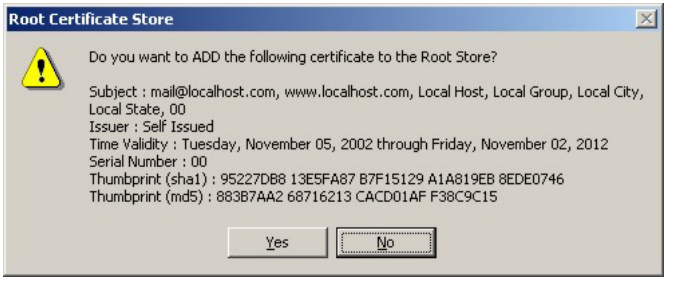


Figure 21-8 Root Certificate Store

Step 8. When the certificate is saved successfully, a **Certificate Import Wizard** window displays. Click **OK**.

Figure 21-9 Certificate Import Wizard

Step 9. A **Certificate** window displays the detail information.

Figure 21-10 Certificate: Details

Step 10. Click **OK** in the **Certificate** window to return to the **Security Alert** window as shown. Notice that the first item in the list changed to inform you that the certificate is from a trusted host. Click **OK** to proceed to the login screen in secure mode.

Figure 21-11 Security Alert: Trusted

21.4 Activating SSL Security for Subscriber Logins

Follow the steps below to activate the SSL security for subscriber login connections to the ZyAIR.

Step 1. Click **ADVANCED**, **AUTHENTICATION** and select **Enable** in the **SSL Login Page Security** field

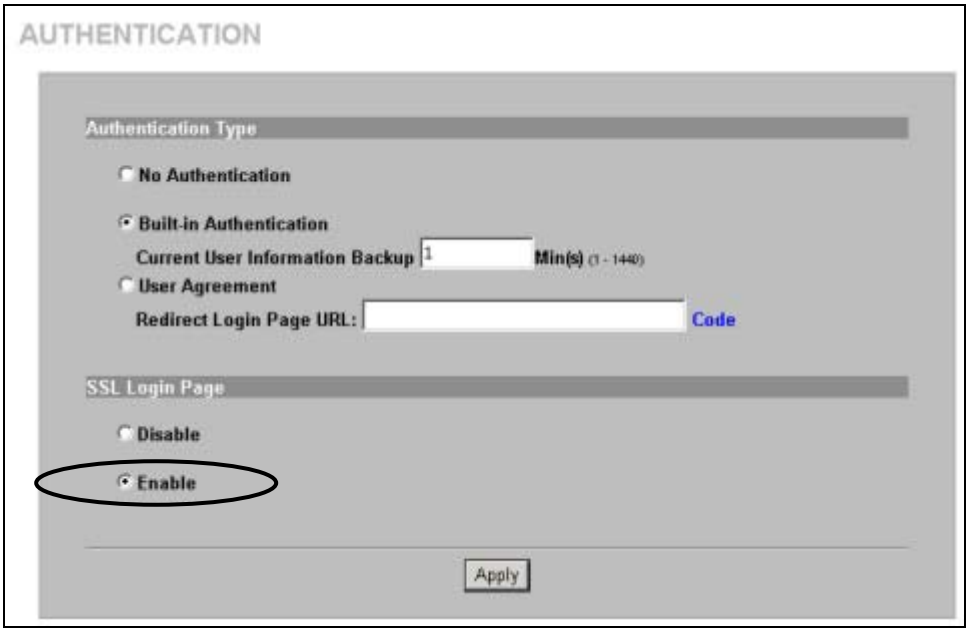


Figure 21-12 AUTHENTICATION: Activate SSL Login

Step 2. Click **Apply** to save the changes and restart the ZyAIR when prompted.

21.5 SSL Certificate Download

You can register for a certificate from a CA (Certificate Authority). A CA issues digital certificates and guarantees the identity of the certificate owner.

Click **SYSTEM TOOLS**, **SSL CERTIFICATE** to open the **SSL CERTIFICATE** screen. Use this screen to download a CA registered certificate from a computer connected to the ZyAIR.

You must save the certificate and private key files from the CA on a computer that is connected to the ZyAIR.

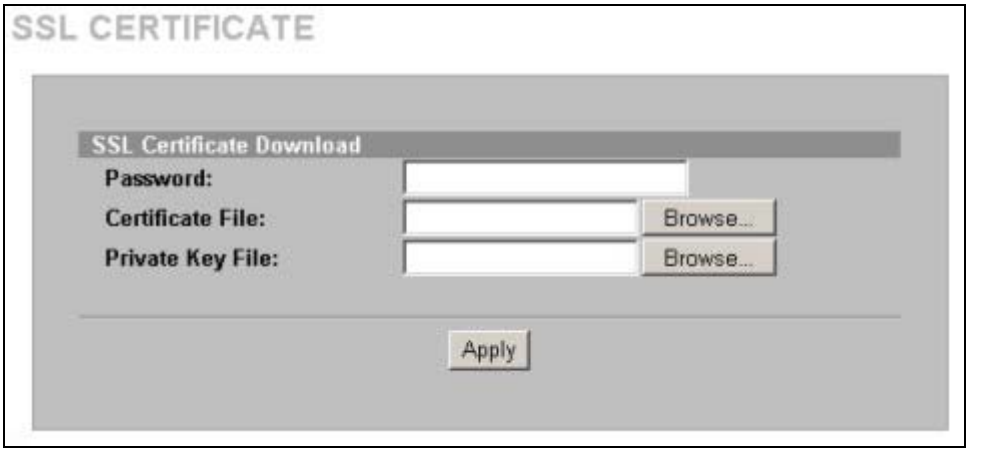


Figure 21-13 SSL CERTIFICATE

The following table describes the labels in this screen.

Table 21-1 SSL CERTIFICATE

LABEL	DESCRIPTION
Password	Enter the private key password from the CA. Make sure you enter it exactly as the CA provides.
Certificate File	Specify the name and/or location of the file containing the certificate. Or click **Browse** to locate the file.
Private Key File	Specify the name and/or location of the file containing the private key, Or click **Browse** to locate the file.
Apply	Click **Apply** to transfer the certificate and private key files from the computer to the ZyAIR.

After you download the certificate files, click **Apply** to restart the ZyAIR.

See the chapter on general system setup for how to set the ZyAIR to use the certificate that you download.

Chapter 22
Ping Command

*This chapter covers how to use the **PING COMMAND** screen.*

22.1 About Ping Command

Use the ping function to check the ZyAIR's network connection.

22.2 Using Ping Command

Click **SYSTEM TOOLS** and then **PING COMMAND** to open the following screen.

The following table describes the labels in this screen.

Table 22-1 PING COMMAND

LABEL	DESCRIPTION
Destination IP Address	Type the IP address of a device that you want to ping in order to test the connection.
Ping	Click this button to have the device ping the IP address.
Clear	Click this button to clear the ping results in the multi-line text box.
Ping Result	This multi-line text box displays the results of the ping.

Chapter 23
Troubleshooting

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

23.1 Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

23.1.1 The Power LED

The **PWR** LED on the front panel does not light up.

Table 23-1 Troubleshooting Power LED

STEPS	CORRECTIVE ACTION
1	Check the connection from the ZyAIR to the power source. Make sure you are using the supplied power supply. Refer to the product specifications.
2	Make sure the power source is turned on and that the ZyAIR is receiving sufficient power.
3	If these steps fail to correct the problem, contact your local distributor for assistance.

23.1.2 The LAN Port LEDs

None of the LEDs for the LAN port(s) light up when connected to an Ethernet device.

Table 23-2 Troubleshooting LAN LEDs

STEPS	CORRECTIVE ACTION
1	Make sure the ZyAIR is turned on.
2	Verify that the attached device(s) is turned on and properly connected to the ZyAIR.
3	Verify that the Ethernet cable length does not exceed 100 meters.
4	Make sure the network adapters are working on the attached device(s).

23.1.3 The WAN Port LED

The LED for the WAN port does not light up when connected to an Ethernet device.

Table 23-3 Troubleshooting WAN LEDs

STEPS	CORRECTIVE ACTION
1	Make sure you connect your cable or DSL modem or router to this port using the Ethernet cable that came with your cable or DSL modem or router.
2	Verify that the attached device is turned on and properly connected to the ZyAIR.
3	Verify that the Ethernet cable length does not exceed 100 meters.

23.2 Web Configurator

I cannot access the web configurator.

Table 23-4 Troubleshooting the Web Configurator

STEPS	CORRECTIVE ACTION
1	Make sure you are using either Internet Explorer (version 4.0 and later) or Netscape Navigator (version 6.0 and later).
2	Make sure you are using the correct WAN or LAN IP address. The default LAN IP address is **192.168.1.1**.
3	Make sure you entered the correct username and password. The default administrator username is “admin” and the default password is “1234”. The username and password are case-sensitive. If you have forgotten the administrator user name and/or password, you must reset the ZyAIR back to the factory defaults using the reset button. Use a pointed object to press the reset button on the side panel to reset the ZyAIR. All of your custom configuration will be lost.
4	Ping the ZyAIR from your computer on the WAN or LAN. If you cannot ping the ZyAIR, check the IP addresses of the ZyAIR and your computer. Make sure that both IP addresses are in the same subnet.
5	Delete the temporary web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.) In Netscape, click **Edit**, **Preference**. Under **Advanced** category, click **Cache**. Click **Clear Memory Cache** and **Clear Disk Cache**. (Steps may vary depending on the version of your Internet browser.)
6	Disable any HTTP proxy settings in your web browser.

The web configurator does not display properly.

Table 23-5 Troubleshooting the Internet Browser Display

STEPS	CORRECTIVE ACTION
1	Make sure you are using either Internet Explorer (version 4.0 or above) or Netscape Navigator (6.0 or above). Make sure that your browser has JavaScript support enabled.
2	Delete the temporary web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.) In Netscape, click **Edit**, **Preference**. Under **Advanced** category, click **Cache**. Click **Clear Memory Cache** and **Clear Disk Cache**. (Steps may vary depending on the version of your Internet browser.)

23.3 Internet Access

A subscriber cannot connect to the Internet through the ZyAIR.

Table 23-6 Troubleshooting Internet Access

STEPS	CORRECTIVE ACTION
1	Check your Internet settings on your modem and/or router.
2	Make sure the subscriber enters the correct user name and password to log in to the ZyAIR. The user name and password are case sensitive.
3	Verify that the IP addresses and the subnet masks of the ZyAIR and the computers are on the same subnet.
4	Make sure the account is still valid.
5	Make sure there is no conflict in IP address assignment. Refer to the appendix.
6	For wireless clients, check that both the ZyAIR and wireless client(s) are using the same ESSID, channel and WEP key (if WEP encryption is activated).

23.4 The Statement Printer

This section is applicable when you use an external statement printer.

I cannot print subscriber statements using the statement printer.

Table 23-7 Troubleshooting the Statement Printer

STEPS	CORRECTIVE ACTION
1	Make sure the statement printer is connected to a power source and is turned on.
2	Check that the statement printer is connected to the port labeled **DEVICE PORT**.
3	Make sure there is enough printing paper in the statement printer.
4	Make sure you set the ZyAIR to require authentication before allowing Internet access, see the Wizard Setup screens or the **Authentication** chapter.

Part VI:

Additional Information

This part provides contains background information on setting up your computer's IP address, IP address assignment conflicts, wireless LAN, PPPoE, PPTP, IP subnetting, subscriber login, and cable types and cable pin assignments. It also provides an index of key terms.

Appendix A
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.

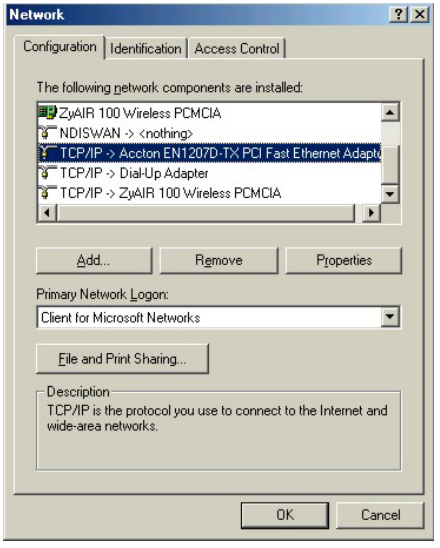
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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**.

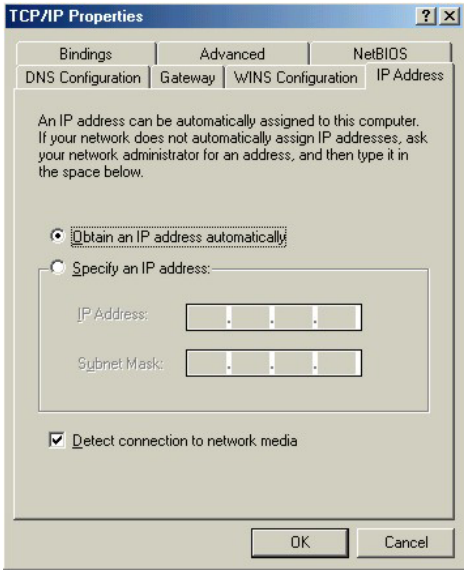
e. Restart your computer so the changes you made take effect.

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**.

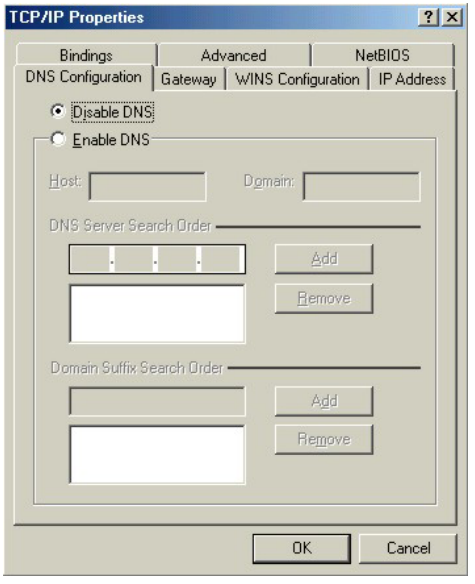
   -If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



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

   -If you do not know your DNS information, select **Disable DNS**.

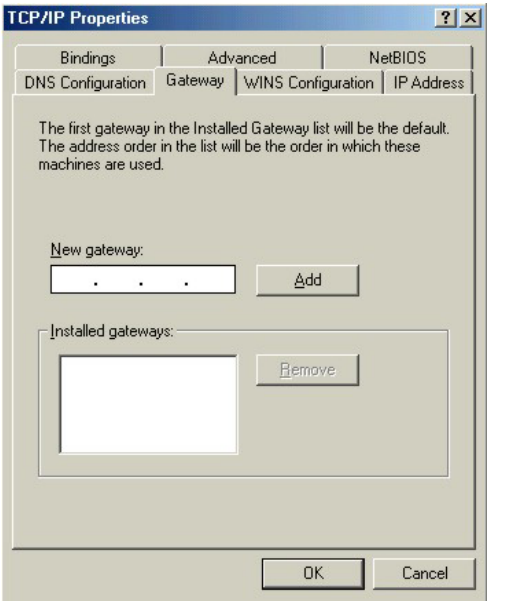
   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



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

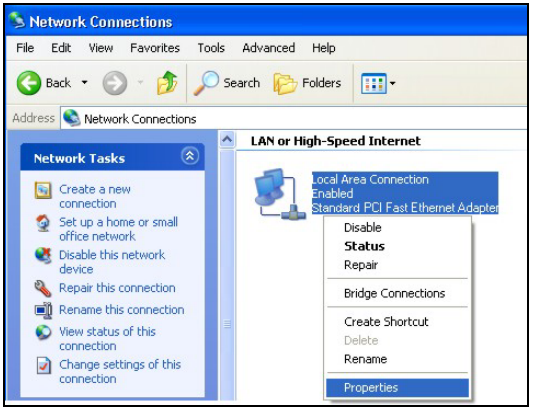
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

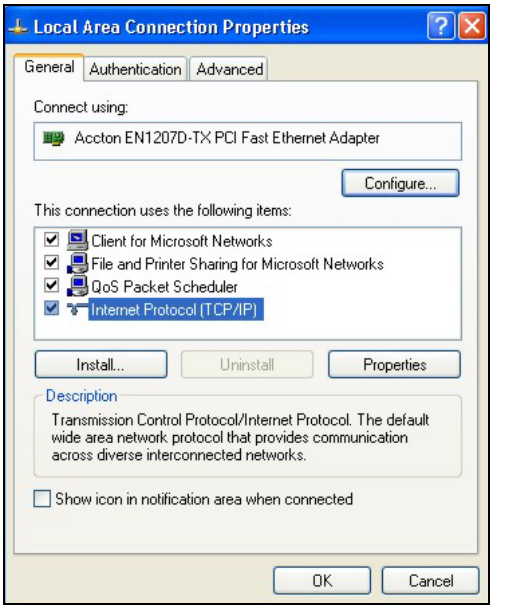
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

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**.

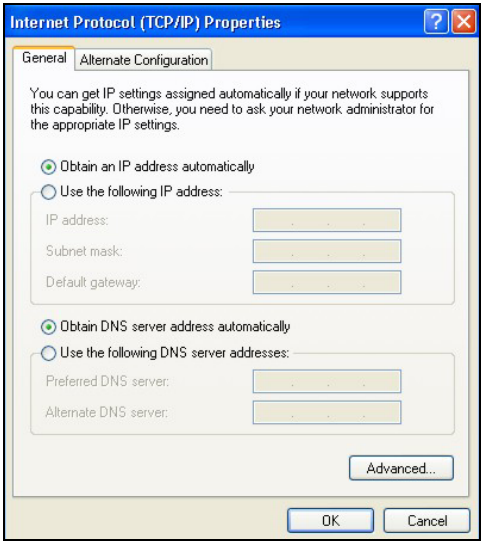


5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

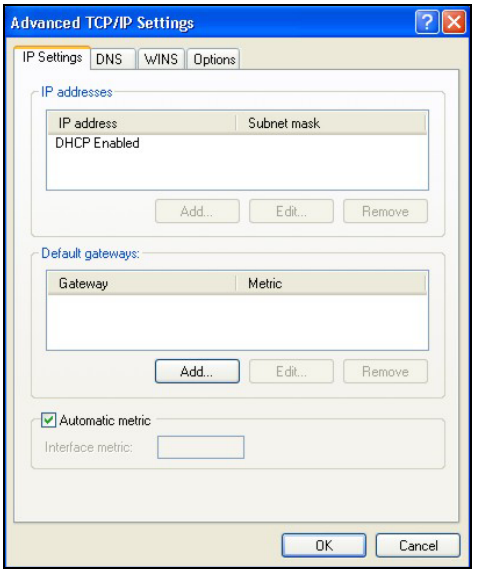
   -If you have a dynamic IP address click **Obtain an IP address automatically**.

   -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 Setting**s tab and click **OK**.



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

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

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

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

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

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

-Click **Add**.

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

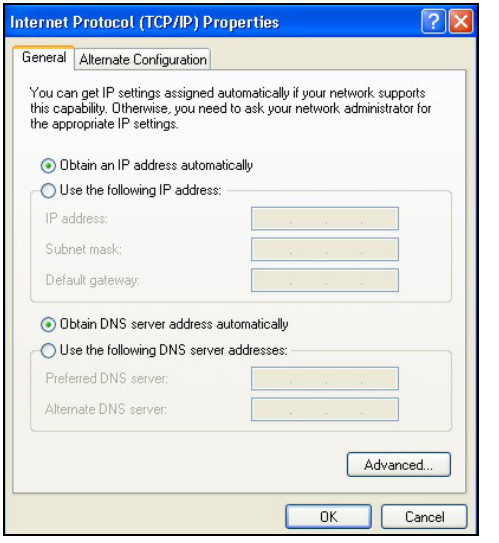
-Click **OK** when finished.

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

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

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

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



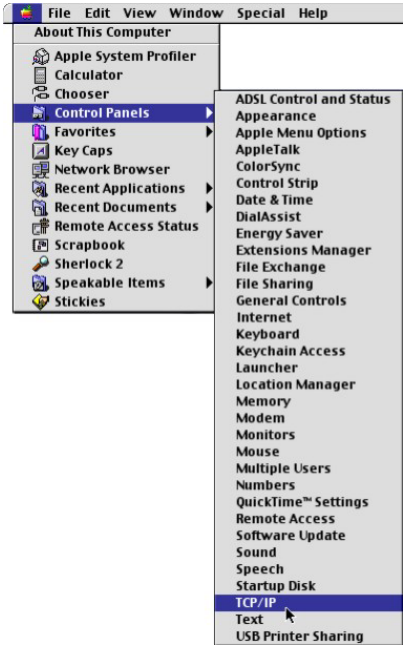
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

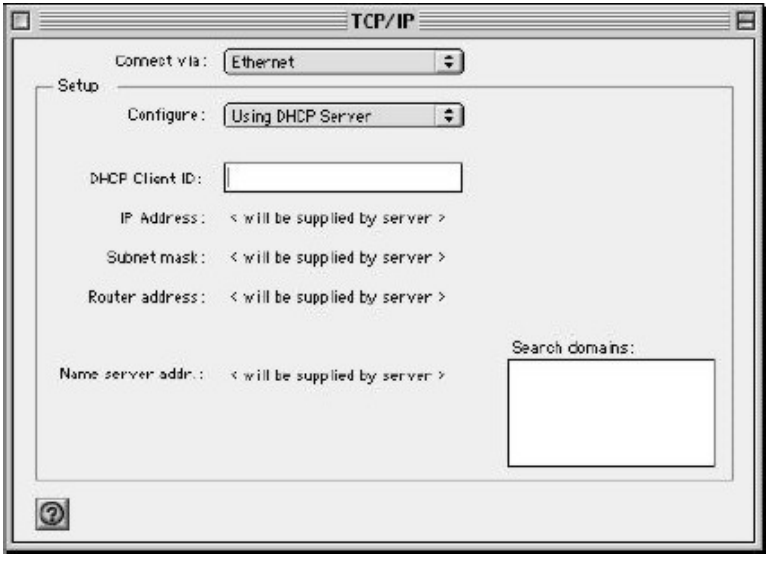
1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

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.

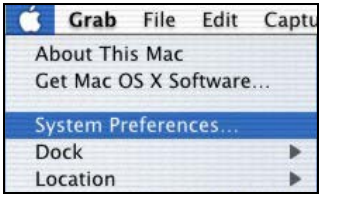
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your ZyAIR and restart your computer (if prompted).

Verifying Your Computer's IP Address

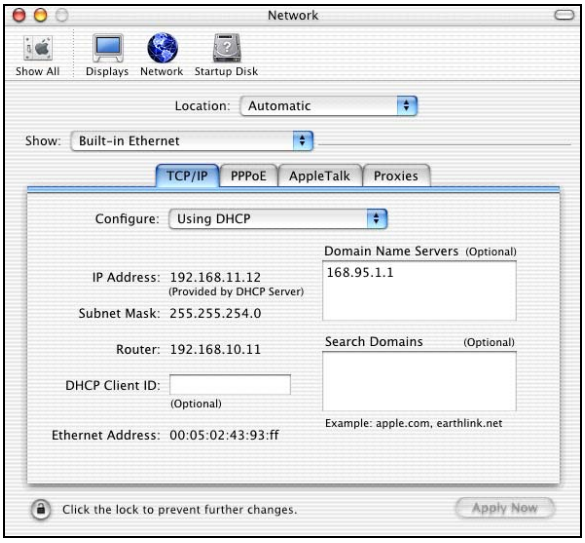
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

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 B
IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

Case A: The ZyAIR is using the same LAN and WAN IP addresses

The following figure shows an example where the ZyAIR is using a WAN IP address that is the same as the IP address of a computer on the LAN.

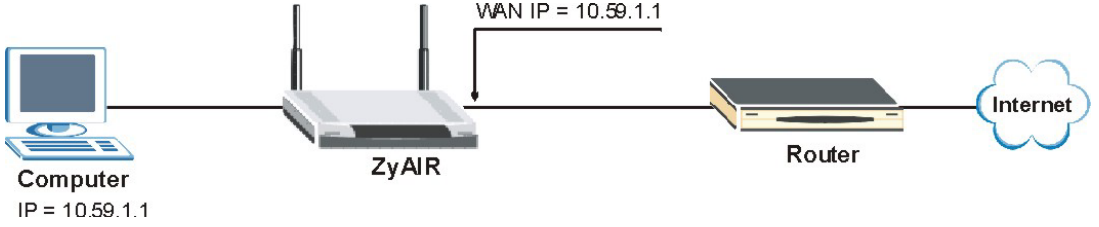


Diagram B-1 IP Address Conflicts: Case A

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

Case B: The ZyAIR LAN IP address conflicts with the DHCP client IP address

In the following figure, the ZyAIR is acting as a DHCP server. The ZyAIR assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

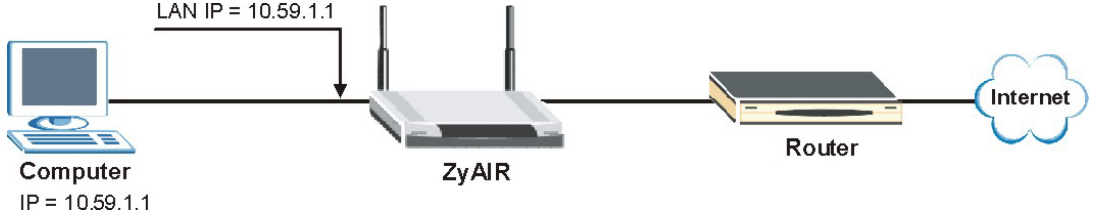


Diagram B-2 IP Address Conflicts: Case B

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

Case C: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the ZyAIR.

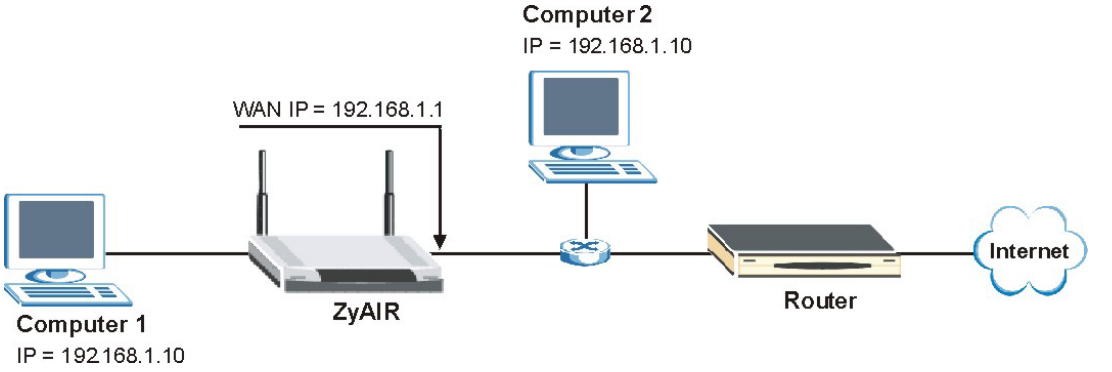


Diagram B-3 IP Address Conflicts: Case C

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

Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the ZyAIR allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the ZyAIR DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.

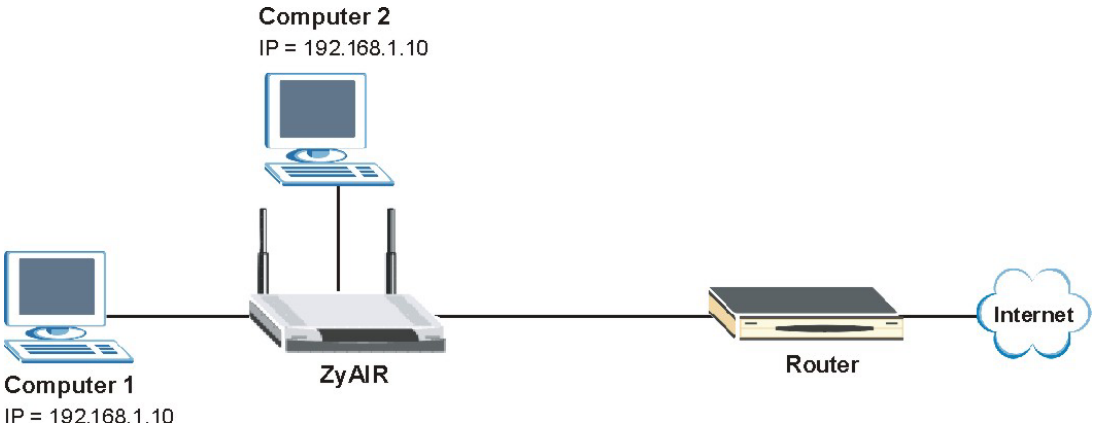


Diagram B-4 IP Address Conflicts: Case D

This problem can be solved by adding a VLAN-enabled switch or set the computers to obtain IP addresses dynamically.

Appendix C
Wireless LAN and IEEE 802.11

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

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

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

IEEE 802.11

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

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

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

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.

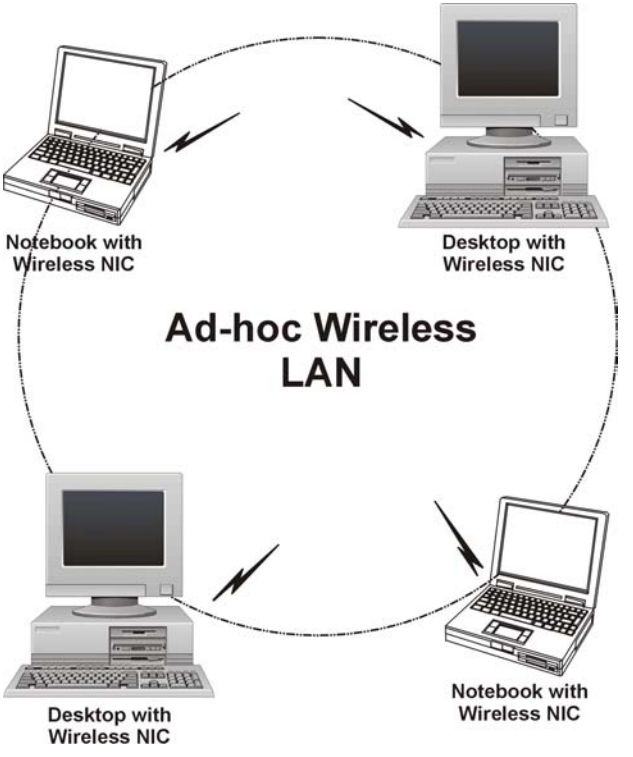


Diagram C-1 Peer-to-Peer Communication in an Ad-hoc Network

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.

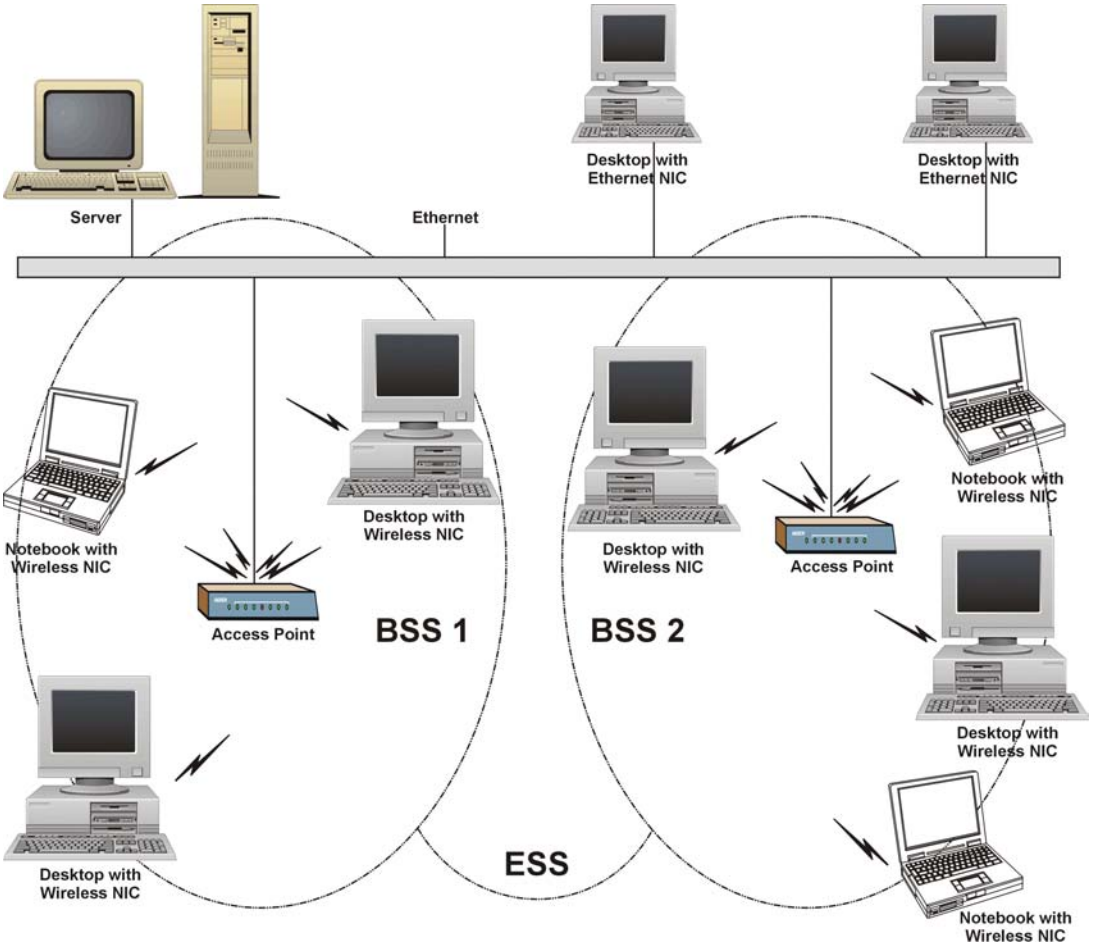


Diagram C-2 ESS Provides Campus-Wide Coverage

Appendix D
Antenna Selection and Positioning Recommendation

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

➢ Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

➢ Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

➢ Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.

- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to –point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Connector Type

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

Appendix E
PPPoE

PPPoE in Action

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

Benefits of PPPoE

PPPoE offers the following benefits:

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

Traditional Dial-up Scenario

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

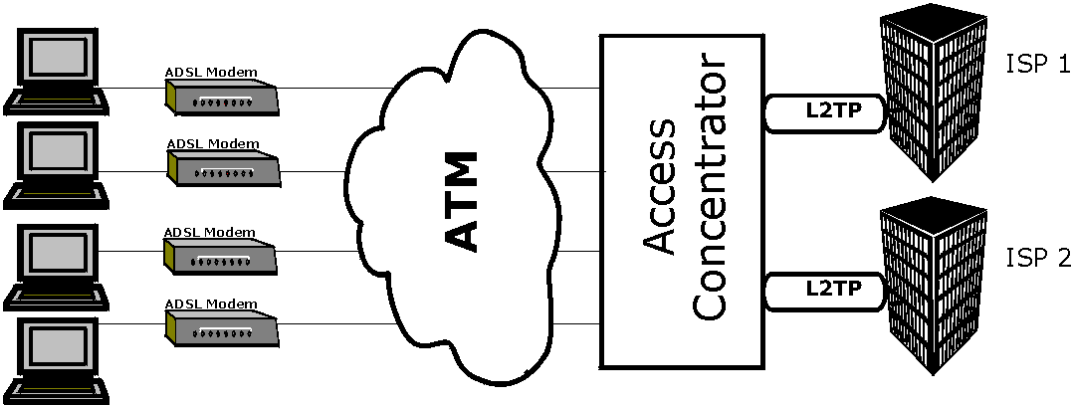


Diagram E-1 Single-PC per Modem Hardware Configuration

How PPPoE Works

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

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

ZyAIR as a PPPoE Client

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

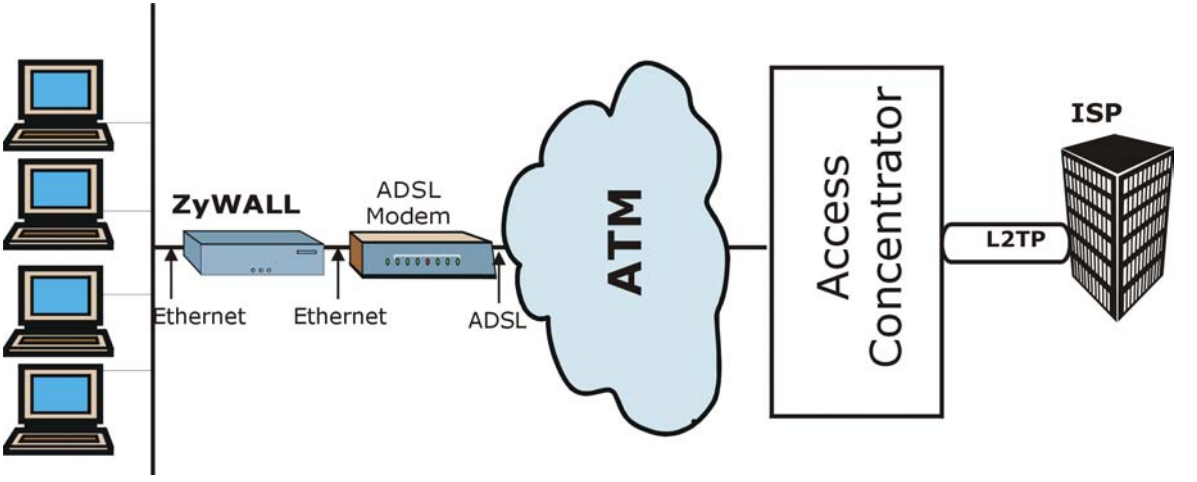


Diagram E-2 ZyAIR as a PPPoE Client

Appendix F
PPTP

What is PPTP?

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

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

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

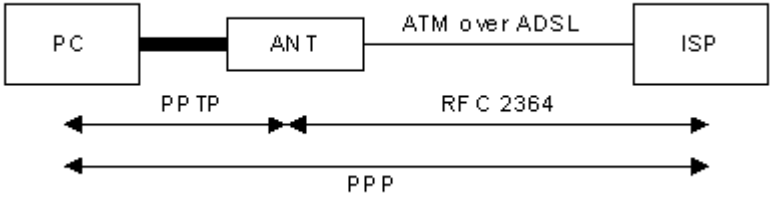


Diagram F-1 Transport PPP frames over Ethernet

PPTP and the ZyAIR

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

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

PPTP Protocol Overview

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

Diagram F-2 PPTP Protocol Overview

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

Control & PPP connections

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

Call Connection

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

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

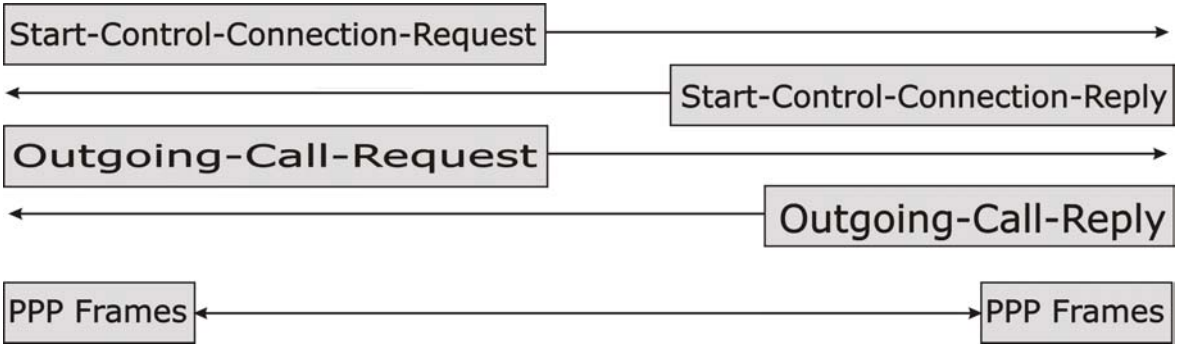


Diagram F-3 Example Message Exchange between PC and an ANT

PPP Data Connection

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

Appendix 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

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 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

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

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

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

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

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

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

Chart 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

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart G-6 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

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

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned

to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart G-7 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Chart G-8 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart G-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Chart G-10 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

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

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

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

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix H
Subscriber Login

To log in as a subscriber, enter a web site address such as www.zyxel.com in a web browser.

If user authentication is activated, the login screen displays prompting you to enter the user name and password. A standard subscriber login screen (with the credit card function) is shown in the figure below.

Diagram H-1 Subscriber Login Screen

Enter a user name and password and click **Enter**. Depending on the settings in the ZyAIR, either the specified web page or an advertisement web page displays. A **Time Window** screen also displays showing the amount of time remaining on the account for Internet access.

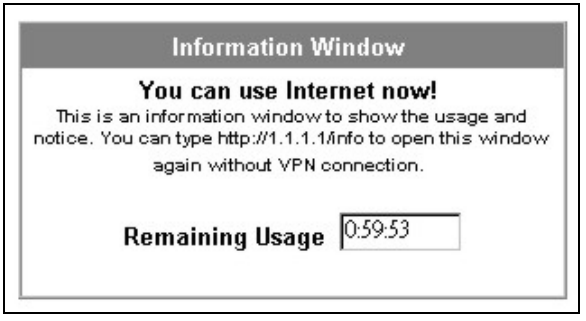


Diagram H-2 Subscriber Login: Time Windows

Appendix I
Cable Types and Cable Pin Assignments

RJ-45 Ethernet Port

The following table describes the types of network cable used for the different connection speeds.

Make sure the Ethernet cable length between connections does not exceed 100 meters (328 feet).

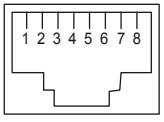
Chart I-1Network Cable Types

SPEED	NETWORK CABLE TYPE
10 Base-TX	100Ω 2-pair UTP/STP Category 3, 4 or 5
100 Base-TX	100Ω 2-pair UTP/STP Category 5

The WAN Port

The following table describes the Ethernet cable pin assignments for the WAN port.

Chart I-2 WAN Port Cable Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
	1	Output Transmit Data +	TD+
	2	Output Transmit Data -	TD-
	3	Input Transmit Data +	RD+
	4	Unused	N/U
	5	Unused	N/U
	6	Input Transmit Data -	RD-
	7	Unused	N/U
	8	Unused	N/U

Make sure that the Ethernet cable connection between the ZyAIR and the hub or router conforms to the following pin assignments.

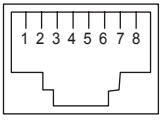
Chart I-3 WAN Port Cable Pin Assignments

ETHERNET DEVICE (SWITCH/HUB/ROUTER ETC.)			ZYAIR	
1	RD+	———	1	TD+
2	RD-	———	2	TD-
3	TD+	———	3	RD+
6	TD-	———	6	RD-

The LAN Port

The following table describes the Ethernet cable pin assignments for the LAN port.

Chart I-4 LAN Port Cable Pin Assignments



PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
1	Input Transmit Data +	RD+
2	Input Transmit Data -	RD-
3	Output Transmit Data +	TD+
4	Unused	N/U
5	Unused	N/U
6	Output Transmit Data -	TD-
7	Unused	N/U
8	Unused	N/U

Make sure that the Ethernet cable connection between the ZyAIR and a computer or switch uplink port conforms to the following pin assignments.

Chart I-5 LAN Port Cable Pin Assignments

ETHERNET DEVICE (COMPUTER/ UPLINK PORT)			ZYAIR	
1	TD+	———	1	RD+
2	TD-	———	2	RD-
3	RD+	———	3	TD+
6	RD-	———	6	TD-

The DEVICE Port

The following table describes the printer cable pin assignments that the ZyAIR's device port uses with the exclusive printer.

Chart I-6 Device Port Cable Pin Assignments

ZYAIR DB25		EXCLUSIVE PRINTER RJ-11
2	———	2
3	———	3
7	———	4
5	———	5

Appendix J Index

A

Account Manager Account 2-8

Account Printout 10-12

Account printout preview.... 10-15, 10-18, 10-21, 10-24

Accumulation 6-1

Ad-hoc Configuration C-2

Administrator Account 2-8

Advertisement Links 14-2

Alternative Subnet Mask Notation G-3

Antenna 1-4

Directional D-2

Omni-directional D-1

Types D-1

Antenna gain D-1

Applications 1-5

auto-negotiation 1-4

B

Basic Service Set C-2

BSS ..... See Basic Service Set

C

Cable

Pin assignments I-1

Changing System password 2-8

Classes of IP Addresses G-1

Computer's IP Address A-1

Configuration and Firmware Files

Filename Convention 20-1

Configuration file

backup 20-1, 20-3

restore 20-5, 20-6

Copyright ii

Coverage 1-4

Credit Card 10-17

Current Users 19-7

Customer Support v

D

Data encryption 18-3

Default LAN IP address 4-1

DHCP 1-2

DHCP client 4-1

DHCP Client Table 19-8

Direct Sequence Spread Spectrum C-2

Distribution System C-3

Domain Name System 4-2

DS ..... See Distribution System

DSSS ..... See Direct Sequence Spread Spectrum

Dynamic DNS 15-1
Dynamic Host Configuration Protocol 4-1
DYNDNS Wildcard 15-1

E

Encapsulation
PPP over Ethernet E-1
ESS ..... See Extended Service Set. See Extended Service Set
Ethernet 4-3
Ethernet Cable
Types I-1
Ethernet Cable Length Limit I-1
Ethernet Cable Types I-1
Extended Service Set C-3, 18-2
Extended Service Set IDentification 18-7

F

Factory Ethernet Defaults 4-1
FCC iii
Features 1-1
FHSS. See Frequency-Hopping Spread Spectrum
Filename Convention
Note for web configurator 20-1
Firmware Upgrade 20-7
Fragmentation Threshold 18-5
Frequency-Hopping Spread Spectrum C-2

H

Host IDs G-1

I

IANA 4-2
IBSS ..... See Independent Basic Service Set
IEEE 802.11 ..... C-1
IEEE 802.1Q Tagged VLAN 1-1
Independent Basic Service Set C-2, 18-1
Infrastructure Configuration C-3
Internet Access 1-2
Internet Assigned Numbers Authority .See IANA
IP Address 4-2
IP Address Assignment 4-1
IP Address Assignment Conflicts B-1
IP Addresses
Private 4-2
IP Addressing G-1
IP Classes G-1

L

LAN device 16-1
accessing 19-11
detecting Time 16-2
LAN Device
Port Mapping 16-1
LAN device management 16-1
LAN Devices 19-10
Login Name 15-3

M

Manual Entry 18-9

Manual firmware upgrade
using TFTP....20-8
N
NAT 4-3
NAT (Network Address Translation - NAT, RFC 1631) 16-1
Network Cable Types
100Mbps I-1
10Mbps I-1
P
Passthrough 11-1
Ping Command....22-1
Point-to-Point Tunneling Protocol 4-4
Portal page 14-1
PPPoE 4-3
PPTP F-1, 4-4
PPTP Support....1-2
Preamble Mode 18-5
Long....18-5
Short....18-5
Private IP Addresses 4-2
Q
Quick Installation Guide xix
R
Related Documentation....xix
Restarting the ZyAIR....2-13
Reverse SMA connectors....1-4
RF signals....C-1
RTS Threshold 18-3
S
Server port....16-1
Service....iv
Service Set....18-7
Subnet Mask....4-2
Subnet Masks G-2
Subnetting G-2
Subscriber information window 10-10
Subscriber Login H-1
Super Subscriber Account....2-8
Supervisor Account....2-8
Supporting Disk xix
T
Troubleshooting 23-1
Internet Access....23-3
Internet Browser Display 23-3
LAN LEDs 23-1
Power LED....23-1
the Account Generator 23-4
WAN LEDs....23-2
Web configurator 23-2
Type of system login accounts
account manager....2-8
administrator 2-8
Types of Login Accounts 2-8

U
Using LEDs To Diagnose Problems 23-1
V
View Current Configuration 19-1
Virtual port 16-1
W
Wall Garden 14-3
Web configurator 2-1
accessing 2-1
Web Configurator
Screens Overview 2-4
Supported Browsers 2-1
WEP 18-3
Wireless LAN C-1
Benefits C-1
Wizard Setup 2-2
WLAN ..... See Wireless LAN
Z
ZyXEL Limited Warranty
Note iv