G-4100 v2

802.11g Wireless Hotspot Gateway

User's Guide

Version 1.00
7/2006
Edition 1

Downloaded from www.Manualslib.com manuals search engine

FreeWheel, Ex. 1085
FreeWheel v. AlmondNet
IPR2024-00419

Downloaded from www.Manualslib.com manuals search engine

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

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

Downloaded from www.Manualslib.com manuals search engine

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

FCC Radiation Exposure Statement

- The device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2). End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用

Downloaded from www.Manualslib.com manuals search engine

者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Notices

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

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

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

Viewing Certifications

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

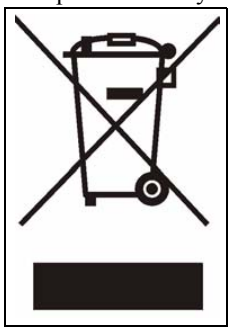
Downloaded from www.Manualslib.com manuals search engine

Safety Warnings

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

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Connect the power cord to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.

This product is recyclable. Dispose of it properly.



Downloaded from www.Manualslib.com manuals search engine

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.

Registration

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.

Downloaded from www.Manualslib.com manuals search engine

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[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		

Downloaded from www.Manualslib.com manuals search engine

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
POLAND	info@pl.zyxel.com	+48 (22) 333 8250 +48 (22) 333 8251	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
RUSSIA	http://zyxel.ru/support sales@zyxel.ru	+7-095-542-89-29 +7-095-542-89-25	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
SPAIN	support@zyxel.es sales@zyxel.es	+34-902-195-420 +34-913-005-345	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 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
UKRAINE	support@ua.zyxel.com sales@ua.zyxel.com	+380-44-247-69-78 +380-44-494-49-32	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
UNITED KINGDOM	support@zyxel.co.uk sales@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only) +44-1344 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)

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

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Table of Contents

Copyright 3

Certifications 4

Safety Warnings 6

ZyXEL Limited Warranty 7

Customer Support 8

Table of Contents 11

List of Figures 19

List of Tables 23

Preface 27

Chapter 1
Getting to Know Your ZyXEL Device 29

1.1 Introducing the ZyXEL Device 29
1.2 Features 29
1.3 Applications 33
1.3.1 Internet Access for LAN Networks 33
1.3.2 Internet Access in Public Areas 34

Chapter 2
The Web Configurator 35

2.1 Introducing the Web Configurator 35
2.2 Accessing the Web Configurator 35
2.3 Wizard Setup Screens 36
2.4 Navigating the Web Configurator 36
2.5 Screens Overview 38
2.6 Quick View Screen 39
2.7 Login Accounts 41
2.7.1 Changing Login Account Usernames and Passwords 42
2.8 Methods of Restoring Factory-Defaults 44
2.8.1 Using the Reset Button to Restore Factory-Defaults 44
2.8.2 Using the Web Configurator to Restore Factory-Defaults 45
2.9 Restarting the ZyXEL Device 46
2.10 Logging Out of the Web Configurator 47

Downloaded from www.Manualslib.com manuals search engine

Chapter 3
General System Setup 49

3.1 General System Setup 49
3.2 System Name 49
3.3 Domain Name 49
3.4 iPnP ZyXEL Implementation 49
3.4.1 How iPnP Works 50
3.5 General System Settings 51

Chapter 4
WAN, LAN and Server Setup 57

4.1 Factory Ethernet Defaults 57
4.2 LANs and WANs 57
4.3 IP Address Assignment 57
4.4 DHCP Configuration 57
4.4.1 IP Address and Subnet Mask 58
4.4.2 Private IP Addresses 58
4.5 DNS Server Address 59
4.6 PPPoE 59
4.6.1 PPP MTU 59
4.6.2 TCP MSS 60
4.7 PPTP 60
4.8 Configuring the WAN and LAN Settings 60
4.9 Server Configuration 63

Chapter 5
Authentication 67

5.1 About the Built-in Authentication 67
5.2 Authentication Settings 67

Chapter 6
RADIUS 71

6.1 About RADIUS 71
6.2 RADIUS Settings 71

Chapter 7
Billing 75

7.1 About the Built-in Billing 75
7.1.1 Accumulation Accounting Method 75
7.1.2 Time-to-finish Accounting Method 75
7.2 Billing Settings 75

Downloaded from www.Manualslib.com manuals search engine

Chapter 8
Accounting 79

8.1 About Subscriber Accounts 79
8.2 Discount Price Plan 79
8.2.1 Charge by Levels 79
8.3 Accounting Settings 79
8.3.1 Charge By Levels Example 82
8.4 Creating Accounts 83
8.4.1 Creating Accounts in the Web Configurator 83
8.4.2 Using an Exclusive Printer to Create and Print Subscriber Statements ..85
8.5 Viewing the Account List 85

Chapter 9
Credit Card..... 89

9.1 About the Credit Card Screen 89
9.2 Credit Card Settings 89

Chapter 10
Keypad 93

10.1 About the Keypad 93
10.2 Keypad Settings 93
10.3 Keypad Configuration Examples 95
10.3.1 Keypad with Pre-Paid Billing Example 95
10.3.2 Keypad with Post-Paid Billing Example 97

Chapter 11
Customization 101

11.1 About the Customization Screens 101
11.2 About the Login Page Screen 101
11.3 Customizing the Subscriber Login Screen 101
11.3.1 Standard Subscriber Login Screen 102
11.3.2 Redirect Subscriber Login Screen 104
11.3.3 Advanced Subscriber Login Screen 105
11.3.4 Framed Subscriber Login Screen 108
11.4 Adding a Logo 109
11.5 About the Information Windows 110
11.5.1 Customizing the Information Windows 111
11.6 About the Account Printout 112
11.6.1 Customizing the Account Printout 112
11.7 Customizing the Credit Card 118
11.7.1 Credit Card Standard Login Page 118
11.7.2 Credit Card Service Selection Page 119
11.7.3 Credit Card Successful Page 123

Downloaded from www.Manualslib.com manuals search engine

11.7.4 Credit Card Fail Page 125

Chapter 12
Pass Through 127

12.1 About the Pass Through 127
12.2 Configuring Pass Through 127

Chapter 13
Filtering 131

13.1 About Filtering 131
13.2 Configuring Filtering 131

Chapter 14
Share 135

14.1 About Share 135
14.2 Configuring Share 135

Chapter 15
Portal Page, Advertisement Links and Walled Garden 139

15.1 Portal Page Advertisement Links and Walled Garden Overview 139
15.2 Portal Page 139
15.3 Advertisement Links 140
15.4 Walled Garden 141
15.4.1 Walled Garden Login Example 142

Chapter 16
DDNS 143

16.1 About DDNS 143
16.1.1 DYNDNS Wildcard 143
16.2 Configuring DDNS 143

Chapter 17
LAN Devices 147

17.1 LAN Devices and NAT Overview 147
17.1.1 Port Mapping 147
17.2 Configuring LAN Devices Port Mapping 147
17.2.1 LAN Device Management Example 149
17.2.2 Specifying an Inside Server Example 150

Chapter 18
Syslog 153

18.1 Syslog Configuration 153
18.2 Syslog Log Settings Configuration 155

Downloaded from www.Manualslib.com manuals search engine

Chapter 19
Session Trace 161

19.1 Session Trace 161
19.2 Session Trace Configuration 161
19.3 Session Trace Filename Convention 162

Chapter 20
Bandwidth 165

20.1 Bandwidth 165
20.2 Bandwidth Configuration 165

Chapter 21
Secure Remote 167

21.1 Secure Remote Configuration 167

Chapter 22
Account Generator 169

22.1 Account Generator Configuration 169

Chapter 23
Wireless LAN 173

23.1 Wireless LAN Overview 173
23.1.1 IBSS 173
23.1.2 BSS 173
23.1.3 ESS 174
23.2 Wireless LAN Basics 174
23.2.1 Wireless Standards 175
23.2.2 Wireless LAN Coverage 175
23.2.3 Channel 175
23.2.4 Introduction to WPA 176
23.2.5 WEP Encryption 176
23.2.6 RTS/CTS 176
23.2.7 Fragmentation Threshold 177
23.3 Wireless LAN Setup 178

Chapter 24
Subscriber Login 183

Chapter 25
Report Printing Using the SP-200E 185

25.1 Reports Overview 185
25.2 Key Combinations 185
25.3 Daily Account Summary 186

Downloaded from www.Manualslib.com manuals search engine

25.4 Monthly Account Summary 186
25.5 Account Report Notes 187
25.6 System Status 187
25.7 Network Statistics 189

Chapter 26
System Status..... 191

26.1 About System Status 191
26.2 View System Information 191
26.3 Account List 194
26.4 Account Log 195
26.5 Current Users 196
26.6 DHCP Clients 197
26.7 Session List 197
26.8 LAN Devices 199
26.8.1 Accessing a LAN Device 199

Chapter 27
Configuration, Firmware and Accounting Log Maintenance 201

27.1 Filename Conventions 201
27.2 Configuration File Maintenance 201
27.2.1 Backup Configuration Using HTTP 201
27.2.2 Backup Configuration Using TFTP 203
27.2.3 Restore Configuration Using HTTP 204
27.2.4 Restore Configuration Using TFTP 204
27.3 Firmware Upgrade 205
27.3.1 Manual Firmware Upgrade Using the Web Configurator 206
27.3.2 Manual Firmware Upgrade via TFTP Server 207
27.3.3 Manual Boot Code Upgrade Using the Web Configurator 207
27.3.4 Scheduled Firmware Upgrade 209

Chapter 28
SSL (Secure Socket Layer) Security 211

28.1 About SSL 211
28.2 Activating SSL Security for Management Connections 211
28.3 Viewing and Installing the SSL Security Certificate 212
28.4 Activating SSL Security for Subscriber Logins 217
28.5 SSL Certificate Download 218

Chapter 29
Ping Command..... 221

29.1 About Ping Command 221
29.2 Using Ping Command 221

Downloaded from www.Manualslib.com manuals search engine

Chapter 30
Restart 223

30.1 Restart 223

Chapter 31
Troubleshooting 225

31.1 Using LEDs to Diagnose Problems 225
31.1.1 The Power LED 225
31.1.2 The LAN Port LEDs 225
31.1.3 The WAN Port LED 226
31.2 Web Configurator 226
31.3 Internet Access 227
31.4 Statement Printer 227

Appendix A
Product Specifications 229

Appendix B
Setting up Your Computer's IP Address 235

Appendix C
IP Address Assignment Conflicts 251

Appendix D
Indoor Installation Recommendations 255

Appendix E
Wireless LANs 257

Appendix F
IP Addresses and Subnetting 267

Index 275

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

List of Figures

Figure 1 Application: Internet Access for LAN Networks 34
Figure 2 Application: Internet Access in Public Areas 34
Figure 3 Entering ZyXEL Device IP Address in Internet Explorer 35
Figure 4 Web Configurator: Login 36
Figure 5 Web Configurator Navigation 37
Figure 6 WIZARD Submenu 38
Figure 7 Quick View 40
Figure 8 SYSTEM TOOLS > SYSTEM ACCOUNT 43
Figure 9 Side Panel 45
Figure 10 SYSTEM TOOLS > CONFIGURATION 46
Figure 11 Restart 47
Figure 12 LOGOUT 47
Figure 13 iPnP Example 50
Figure 14 ADVANCED > SYSTEM 52
Figure 15 ADVANCED > WAN/LAN 61
Figure 16 ADVANCED > SERVER 64
Figure 17 ADVANCED > AUTHENTICATION 67
Figure 18 ADVANCED > AUTHENTICATION > Code 69
Figure 19 ADVANCED > RADIUS 72
Figure 20 ADVANCED > BILLING 76
Figure 21 ADVANCED > ACCOUNTING 80
Figure 22 Charge By Levels Example 82
Figure 23 Account Generator Panel 83
Figure 24 Web-based Account Generator Printout Preview Example 84
Figure 25 Web-based PC-connected Printout Preview Example 85
Figure 26 Account List 86
Figure 27 ADVANCED > CREDIT CARD 90
Figure 28 ADVANCED > KEYPAD 94
Figure 29 Select Pre-Paid Billing 95
Figure 30 Define Pre-Paid Billing Profiles 96
Figure 31 Billing Profiles 1 and 2 Examples 97
Figure 32 Select Post-Paid Billing 98
Figure 33 Define Post-Paid Billing Plan 98
Figure 34 Post-Paid Account Printout Example 99
Figure 35 Post-Paid Account Bill Printout Example 99
Figure 36 ADVANCED > CUSTOMIZATION > Login Page 102
Figure 37 ADVANCED > CUSTOMIZATION > Login Page: Standard 103
Figure 38 Login Page Example: Standard 104

Downloaded from www.Manualslib.com manuals search engine

Figure 39 ADVANCED > CUSTOMIZATION > Login Page: Redirect 104
Figure 40 ADVANCED > CUSTOMIZATION > Login Page: Redirect > Code 105
Figure 41 ADVANCED > CUSTOMIZATION > Login Page: Advanced 106
Figure 42 ADVANCED > CUSTOMIZATION > Login Page: Advanced> View Color Grid .. 107
Figure 43 Subscriber Login Screen Example: Advanced 108
Figure 44 ADVANCED > CUSTOMIZATION > Login Page: Frame 108
Figure 45 Subscriber Login Screen Example: Frame 109
Figure 46 ADVANCED > CUSTOMIZATION > Logo 110
Figure 47 ADVANCED > CUSTOMIZATION > Information Windows 111
Figure 48 ADVANCED > CUSTOMIZATION > Account Printout 113
Figure 49 Preview of PC-connected Printer Example 116
Figure 50 Preview of Account Generator Printer Example 117
Figure 51 Preview of Post-Paid Printout Example 118
Figure 52 ADVANCED > CUSTOMIZATION > Credit Card: Standard Login Page 119
Figure 53 Credit Card Standard Login Page Example 119
Figure 54 ADVANCED > CUSTOMIZATION > Credit Card: Service Selection Page 120
Figure 55 Credit Card Service Selection Page Preview 123
Figure 56 ADVANCED > CUSTOMIZATION > Credit Card: Successful Page 124
Figure 57 Credit Card Successful Page Preview 125
Figure 58 ADVANCED > CUSTOMIZATION > Credit Card: Fail Page 126
Figure 59 Credit Card Failed Page Preview 126
Figure 60 ADVANCED > PASS THROUGH 128
Figure 61 ADVANCED > FILTERING 132
Figure 62 ADVANCED > SHARE 136
Figure 63 ADVANCED > PORTAL PAGE 139
Figure 64 ADVANCED > ADVERTISEMENT 140
Figure 65 ADVANCED > WALLED GARDEN 141
Figure 66 Walled Garden Login Example 142
Figure 67 ADVANCED > DDNS 144
Figure 68 ADVANCED > LAN DEVICES 148
Figure 69 LAN Device Remote Management Example 1 149
Figure 70 ADVANCED > LAN DEVICES: Example 1 149
Figure 71 LAN Device Remote Management Example 2 150
Figure 72 ADVANCED > LAN DEVICES: Example 2 150
Figure 73 ADVANCED > SYSLOG 154
Figure 74 ADVANCED > SYSLOG > Log Settings 156
Figure 75 ADVANCED > SESSION TRACE 161
Figure 76 Session Trace Information Example 162
Figure 77 ADVANCED > BANDWIDTH 166
Figure 78 ADVANCED > SECURE REMOTE 167
Figure 79 ADVANCED > ACCOUNT GENERATOR 170
Figure 80 IBSS (Ad-hoc) Wireless LAN 173
Figure 81 Basic Service 174

Downloaded from www.Manualslib.com manuals search engine

Figure 82 Extended Service Set 174
Figure 83 RTS/CTS 177
Figure 84 ADVANCED > WIRELESS 179
Figure 85 Subscriber Login Screen 183
Figure 86 Subscriber Login: Time Window 183
Figure 87 Daily Account Example 186
Figure 88 Monthly Account Example 187
Figure 89 System Status Example 188
Figure 90 Network Statistics Example 190
Figure 91 SYSTEM STATUS > SYSTEM 191
Figure 92 SYSTEM STATUS > ACCOUNT LOG 195
Figure 93 SYSTEM STATUS > CURRENT USER 196
Figure 94 SYSTEM STATUS > DHCP 197
Figure 95 SYSTEM STATUS > Session List 198
Figure 96 SYSTEM STATUS > LAN DEVICES 199
Figure 97 SYSTEM TOOLS > CONFIGURATION: Backup Using HTTP 202
Figure 98 Configuration Backup: File Download 202
Figure 99 Configuration Backup: Save As 203
Figure 100 SYSTEM TOOLS > CONFIGURATION: Backup Using TFTP 203
Figure 101 Configuration Backup: Using TFTP Successful 204
Figure 102 SYSTEM TOOLS > CONFIGURATION: Restore Using HTTP 204
Figure 103 SYSTEM TOOLS > CONFIGURATION: Restore Using TFTP 205
Figure 104 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: Using the Web Configurator 206
Figure 105 System Restart 206
Figure 106 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: via TFTP Server 207
Figure 107 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: Boot Code Upgrade Using the Web Configurator 208
Figure 108 System Restart 208
Figure 109 SYSTEM TOOLS > FIRMWARE > Scheduled Firmware Upgrade 209
Figure 110 Synchronization Check File Example 210
Figure 111 ADVANCED > SERVER: Enable SSL (HTTPS) Security 212
Figure 112 Installing the SSL Security Certificate: First Security Alert 213
Figure 113 Installing the SSL Security Certificate: Second Security Alert 213
Figure 114 Installing the SSL Security Certificate: View Certificate 214
Figure 115 Installing the SSL Security Certificate: Certificate Import Wizard 214
Figure 116 Certificate Import Wizard: Location 215
Figure 117 Certificate Import Wizard: Finish 215
Figure 118 Root Certificate Store 216
Figure 119 Certificate Import Wizard 216
Figure 120 Certificate Details 216
Figure 121 Security Alert: Trusted 217
Figure 122 ADVANCED > AUTHENTICATION: Activate SSL Login 218

Downloaded from www.Manualslib.com manuals search engine

Figure 123 SYSTEM TOOLS > SSL CERTIFICATE 218
Figure 124 SYSTEM TOOLS > PING COMMAND 221
Figure 125 SYSTEM TOOLS > RESTART 223
Figure 126 WAN Port Cable Pin Assignments 232
Figure 127 LAN Port Cable Pin Assignments 233
Figure 128 WIndows 95/98/Me: Network: Configuration 236
Figure 129 Windows 95/98/Me: TCP/IP Properties: IP Address 237
Figure 130 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 238
Figure 131 Windows XP: Start Menu 239
Figure 132 Windows XP: Control Panel 239
Figure 133 Windows XP: Control Panel: Network Connections: Properties 240
Figure 134 Windows XP: Local Area Connection Properties 240
Figure 135 Windows XP: Internet Protocol (TCP/IP) Properties 241
Figure 136 Windows XP: Advanced TCP/IP Properties 242
Figure 137 Windows XP: Internet Protocol (TCP/IP) Properties 243
Figure 138 Macintosh OS 8/9: Apple Menu 244
Figure 139 Macintosh OS 8/9: TCP/IP 244
Figure 140 Macintosh OS X: Apple Menu 245
Figure 141 Macintosh OS X: Network 246
Figure 142 Red Hat 9.0: KDE: Network Configuration: Devices 247
Figure 143 Red Hat 9.0: KDE: Ethernet Device: General 247
Figure 144 Red Hat 9.0: KDE: Network Configuration: DNS 248
Figure 145 **Red Hat 9.0: KDE: Network Configuration: Activate** 248
Figure 146 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 249
Figure 147 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 249
Figure 148 Red Hat 9.0: DNS Settings in resolv.conf 249
Figure 149 Red Hat 9.0: Restart Ethernet Card 250
Figure 150 Red Hat 9.0: Checking TCP/IP Properties 250
Figure 151 IP Address Conflicts: Case A 251
Figure 152 IP Address Conflicts: Case B 252
Figure 153 IP Address Conflicts: Case C 252
Figure 154 IP Address Conflicts: Case D 253
Figure 155 Peer-to-Peer Communication in an Ad-hoc Network 257
Figure 156 Basic Service Set 258
Figure 157 Infrastructure WLAN 259
Figure 158 RTS/CTS 260

Downloaded from www.Manualslib.com manuals search engine

List of Tables

Table 1 Web Configurator Screens Overview 39
Table 2 Quick View 40
Table 3 SYSTEM TOOLS > SYSTEM ACCOUNT 43
Table 4 SYSTEM TOOLS > CONFIGURATION 46
Table 5 ADVANCED > SYSTEM 53
Table 6 ADVANCED > LAN/WAN 62
Table 7 ADVANCED > SERVER 65
Table 8 ADVANCED > AUTHENTICATION 68
Table 9 ADVANCED > RADIUS 73
Table 10 ADVANCED > BILLING 77
Table 11 ADVANCED > ACCOUNTING 81
Table 12 Charge By Levels Example 82
Table 13 Account List 86
Table 14 ADVANCED > CREDIT CARD 90
Table 15 ADVANCED > KEYPAD 94
Table 16 ADVANCED > CUSTOMIZATION > Login Page: Standard 103
Table 17 ADVANCED > CUSTOMIZATION > Login Page: Redirect 104
Table 18 ADVANCED > CUSTOMIZATION > Login Page: Advanced 106
Table 19 ADVANCED > CUSTOMIZATION > Login Page: Frame 108
Table 20 ADVANCED > CUSTOMIZATION > Logo 110
Table 21 ADVANCED > CUSTOMIZATION > Information Windows 111
Table 22 ADVANCED > CUSTOMIZATION > Account Printout 114
Table 23 ADVANCED > CUSTOMIZATION > Credit Card: Standard Login Page 119
Table 24 ADVANCED > CUSTOMIZATION > Credit Card: Service Selection Page 121
Table 25 ADVANCED > CUSTOMIZATION > Credit Card: Successful Page 124
Table 26 ADVANCED > CUSTOMIZATION > Credit Card: Fail Page 126
Table 27 ADVANCED > PASS THROUGH 128
Table 28 ADVANCED > FILTERING 132
Table 29 ADVANCED > SHARE 136
Table 30 ADVANCED > PORTAL PAGE 140
Table 31 ADVANCED > ADVERTISEMENT 141
Table 32 ADVANCED > WALLED GARDEN 142
Table 33 ADVANCED > DDNS 145
Table 34 ADVANCED > LAN DEVICES 148
Table 35 ADVANCED > SYSLOG 154
Table 36 Log Formats 157
Table 37 Subscriber Trace Relationship 159
Table 38 Session Trace File Fields 163

Downloaded from www.Manualslib.com manuals search engine

Table 39 ADVANCED > BANDWIDTH 166
Table 40 ADVANCED > SECURE REMOTE 167
Table 41 ADVANCED > ACCOUNT GENERATOR 170
Table 42 IEEE 802.11b Data Rates and Modulation 175
Table 43 IEEE 802.11g Data Rates and Modulation 175
Table 44 Wireless LAN Coverage 175
Table 45 ADVANCED > WIRELESS 180
Table 46 Report Printing Key Combinations 185
Table 47 System Status 188
Table 48 Network Statistics 190
Table 49 SYSTEM STATUS > SYSTEM 193
Table 50 SYSTEM STATUS > ACCOUNT LOG 195
Table 51 SYSTEM STATUS > CURRENT USER 196
Table 52 SYSTEM STATUS > DHCP 197
Table 53 SYSTEM STATUS > Session List 198
Table 54 SYSTEM STATUS > LAN DEVICES 199
Table 55 SYSTEM TOOLS > SSL CERTIFICATE 219
Table 56 SYSTEM TOOLS > PING COMMANDT 221
Table 57 Troubleshooting Power LED 225
Table 58 Troubleshooting LAN LEDs 225
Table 59 Troubleshooting WAN LEDs 226
Table 60 Troubleshooting the Web Configurator 226
Table 61 Troubleshooting the Internet Browser Display 227
Table 62 Troubleshooting Internet Access 227
Table 63 Troubleshooting a Statement Printer 227
Table 64 Firmware Specifications 229
Table 65 Wireless Specifications 230
Table 66 Hardware Specifications 230
Table 67 Certifications 231
Table 68 Network Cable Types 232
Table 69 WAN Port Cable Pin Assignments 232
Table 70 WAN Port Cable Pin Assignments 232
Table 71 LAN Port Cable Pin Assignments 233
Table 72 LAN Port Cable Pin Assignments 233
Table 73 IEEE 802.11g 261
Table 74 Comparison of EAP Authentication Types 265
Table 75 Wireless Security Relational Matrix 265
Table 76 Classes of IP Addresses 268
Table 77 Allowed IP Address Range By Class 268
Table 78 "Natural" Masks 269
Table 79 Alternative Subnet Mask Notation 269
Table 80 Two Subnets Example 270
Table 81 Subnet 1 270

Downloaded from www.Manualslib.com manuals search engine

Table 82 Subnet 2 271
Table 83 Subnet 1 271
Table 84 Subnet 2 272
Table 85 Subnet 3 272
Table 86 Subnet 4 272
Table 87 Eight Subnets 273
Table 88 Class C Subnet Planning 273
Table 89 Class B Subnet Planning 274

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Preface

Congratulations on your purchase of the ZyXEL Device.

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

Your ZyXEL Device is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your ZyXEL Device for its various applications. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

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

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

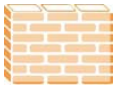
Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Downloaded from www.Manualslib.com manuals search engine

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- Mouse action sequences are denoted using a comma. For example, "In Windows, click **Start**, **Settings** and then **Control Panel**" means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Graphics Icons Key

ZyXEL Device	Computer	Notebook computer
Server	Firewall 	Wireless Signal
Switch	Router	

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 1
Getting to Know Your ZyXEL Device

This chapter introduces the features and applications of the ZyXEL Device.

1.1 Introducing the ZyXEL Device

The ZyXEL Device Hot Spot Gateway combines an IEEE 802.11g wireless access point, router, 4-port switch and service gateway in one box. If you have an "exclusive printer", you can connect it directly to the ZyXEL Device, allowing you to easily print subscriber statements. The ZyXEL Device 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 ZyXEL Device provides the following features to accommodate subscribers with a variety of network configurations with little or no technical support.

iPnP

The IP Plug and Play feature allows a computer to access the Internet or the ZyXEL Device without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.

WEP Data Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private. The ZyXEL Device uses 64-bit or 128-bit WEP encryption.

WPA Data Encryption

Wi-Fi Protected Access (WPA) encrypts data frames before transmitting over the wireless network to help keep network communications private. WPA provides user authentication and better data encryption than WEP.

Downloaded from www.Manualslib.com manuals search engine

VPN (Virtual Private Network) Pass Through

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

VLAN

The ZyXEL Device uses port-based VLAN (Virtual Local Area Network) on the LAN Ethernet ports to block direct communications between subscribers. This is called layer 2 isolation.

SSL Secure Login

With Secure Socket Layer (SSL) activated upon login, data exchanged between the ZyXEL Device 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 ZyXEL Device 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 ZyXEL Device has built-in DHCP server capability. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

E-mail Forwarding

The ZyXEL Device 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 ZyXEL Device provides DNS redirection when a subscriber's configured DNS server is behind a firewall or located in a private Intranet.

Local Subscriber Database

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

RADIUS

The ZyXEL Device can use an external RADIUS (Remote Authentication Dial In User Service defined in RFC2138 and 2139) server for subscriber authentication and accounting.

Accounting

The ZyXEL Device has a built-in accounting feature for keeping track of subscriber Internet usage time.

iPass

The iPass company provides connectivity services for mobile Internet users. The ZyXEL Device can authenticate iPass clients through an external RADIUS server that is Wi-Fi based Wireless Internet Service Provider roaming (WISPr) compliant.

Local Content and Advertising Links

Once connected to the network, the ZyXEL Device 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 ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

Web Configurator Management

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

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version 2c (SNMPv2c).

Upgrade Firmware

The firmware of the ZyXEL Device can be upgraded via the web configurator.

Syslog

The ZyXEL Device'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 ZyXEL Device sends periodically.

IEEE 802.11g Wireless LAN Standard

The ZyXEL Device complies with the IEEE 802.11g wireless standard, which supports data speeds of up to 54 Mbps.

IEEE 802.11b Wireless LAN Standard

The ZyXEL Device is also fully compatible with the 802.11b standard. This means an IEEE 802.11b radio card can interface directly with the ZyXEL Device (and vice versa) at 11 Mbps or lower depending on range.

Antennas

The ZyXEL Device 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.

4-Port Switch

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

Downloaded from www.Manualslib.com manuals search engine

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

This auto-negotiating feature allows the ZyXEL Device 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 ZyXEL Device back to its factory defaults.

Statement Printer

A statement printer allows you to generate subscriber accounts on the ZyXEL Device and print out the account information on-site without using a computer.

The statement printer is also known as an "account generator", "three-button printer" or "exclusive printer".

Ease of Installation

Your ZyXEL Device 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 ZyXEL Device is used. [1]

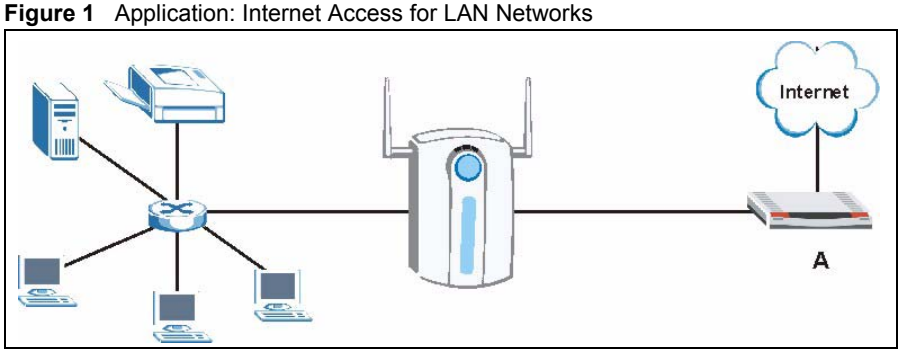
1.3.1 Internet Access for LAN Networks

With a broadband modem or router (A), the ZyXEL Device allows the attached computers to enjoy high speed Internet access.

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

Downloaded from www.Manualslib.com manuals search engine

Figure 1 Application: Internet Access for LAN Networks

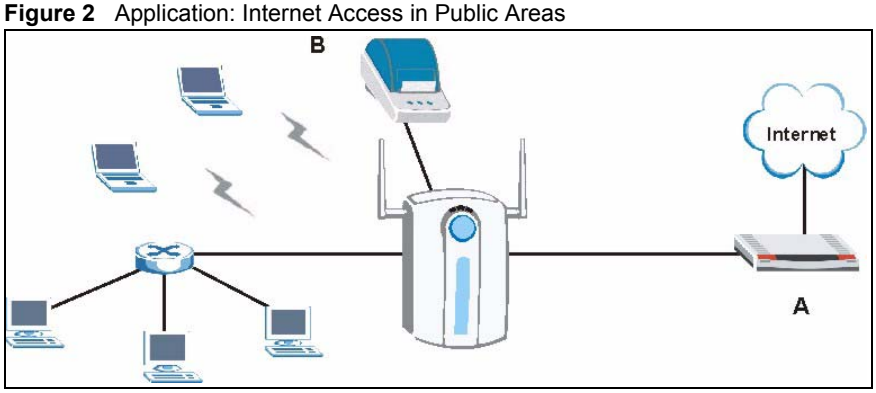


1.3.2 Internet Access in Public Areas

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

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

Figure 2 Application: Internet Access in Public Areas



Downloaded from www.Manualslib.com manuals search engine

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.

Note: The ZyXEL Device allows only one web configurator session at a time.

1. Make sure your ZyXEL Device is properly connected (refer to instructions in the *Quick Start Guide* on hardware installation and connections).
2. Launch your web browser and type the WAN or LAN IP address of the ZyXEL Device 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 separated with a colon ":", for example, http://192.168.1.1:8080.

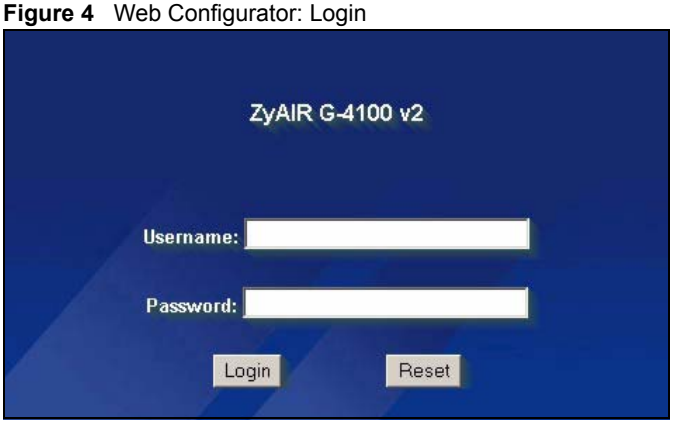
Figure 3 Entering ZyXEL Device IP Address in Internet Explorer

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

Note: The user name and password are case sensitive.

Downloaded from www.Manualslib.com manuals search engine

Figure 4 Web Configurator: Login



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

Note: The ZyXEL Device 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 ZyXEL Device. Refer to the *Quick Start Guide* for information on how to configure the Wizard Setup screens.

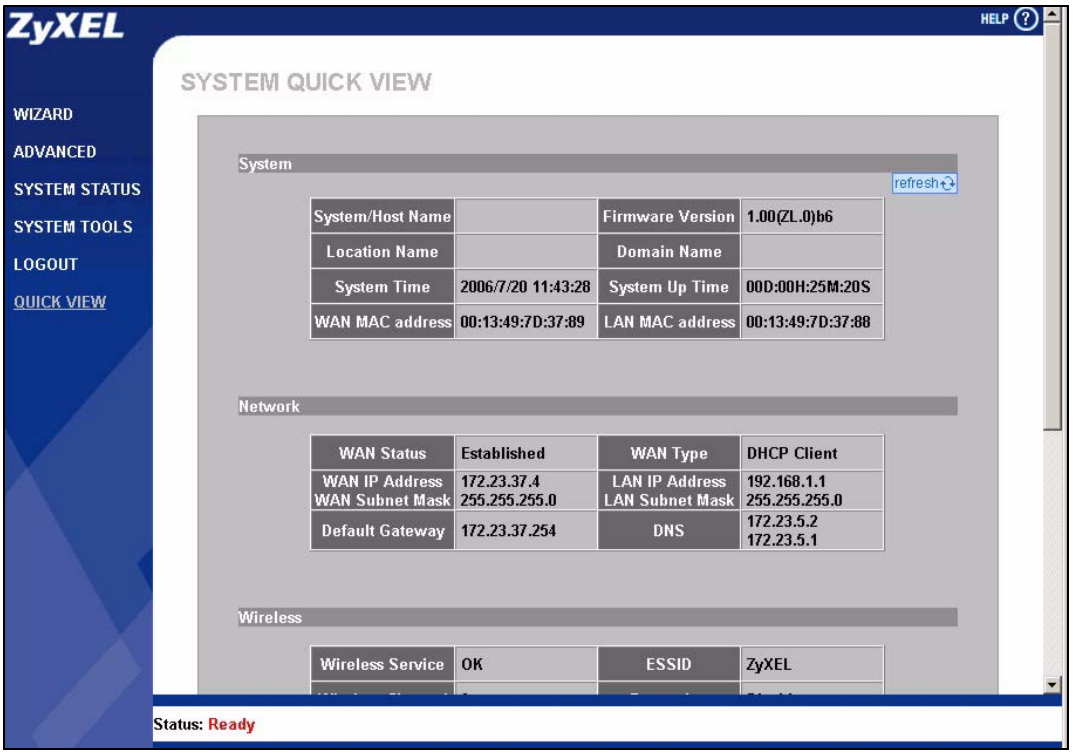
2.4 Navigating the Web Configurator

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

Note: Click the **Help** icon (located in the top right corner of most screens) to view online help.

Downloaded from www.Manualslib.com manuals search engine

Figure 5 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.

Downloaded from www.Manualslib.com manuals search engine

Figure 6 WIZARD Submenu

2.5 Screens Overview

Downloaded from www.Manualslib.com manuals search engine

The following table lists the various web configurator screens.

Table 1 Web Configurator Screens Overview

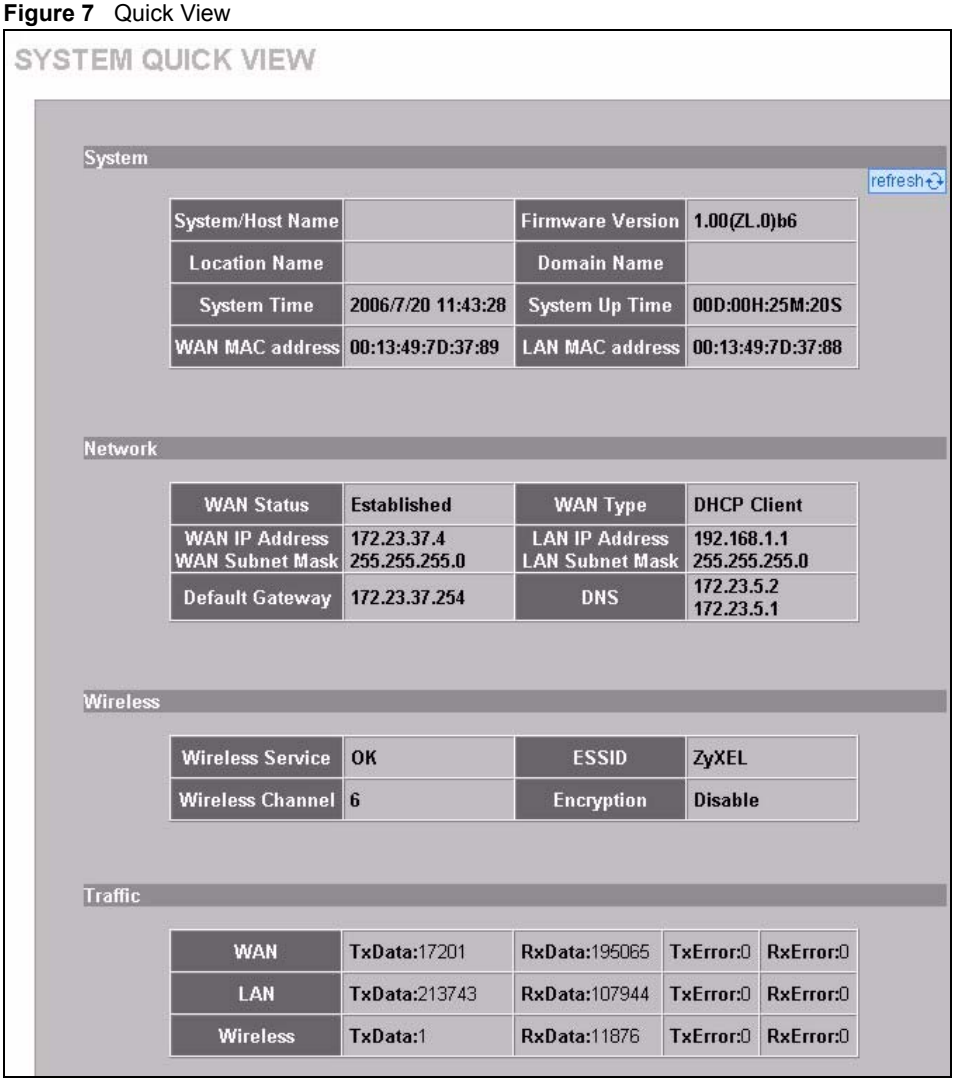
WIZARD	ADVANCED	SYSTEM STATUS	SYSTEM TOOLS
INTERNET WIRELESS E-MAIL AUTHENTICATION BILLING PRINTER ACCOUNTING SYSTEM	SYSTEM WAN/LAN SERVER AUTHENTICATION RADIUS BILLING ACCOUNTING CREDIT CARD KEYPAD CUSTOMIZATION Login Page Logo Information Windows Account Printout Credit Card PASS THROUGH FILTERING SHARE PORTAL PAGE ADVERTISEMENT WALLED GARDEN DDNS LAN DEVICES SYSLOG Syslog Log Settings SESSION TRACE BANDWIDTH SECURE REMOTE ACCOUNT GENERATOR WIRELESS	SYSTEM ACCOUNT LIST ACCOUNT LOG CURRENT USER DHCP CLIENT SESSION LIST LAN DEVICES	CONFIGURATION FIRMWARE Manual Firmware Upgrade Scheduled Firmware Upgrade SYSTEM ACCOUNT SSL CERTIFICATE PING COMMAND RESTART

2.6 Quick View Screen

Click **QUICK VIEW** to display the following screen. This screen displays key system status information.

Downloaded from www.Manualslib.com manuals search engine

Figure 7 Quick View



The following table describes the labels in this screen.

Table 2 Quick View

LABEL	DESCRIPTION
System	
Refresh	Click **Refresh** to update this screen.
System/Host Name	This field displays the description name of the ZyXEL Device for identification purposes.
Firmware Version	This field displays the version of the firmware on the ZyXEL Device.
Location Name	This field displays the device's geographical location.
Domain Name	This field displays the domain name of the ZyXEL Device.

Downloaded from www.Manualslib.com manuals search engine

Table 2 Quick View (continued)

LABEL	DESCRIPTION
System Time	This field displays the ZyXEL Device's current time.
System Up Time	This field displays the how long the ZyXEL Device has been operating since it was last started.
WAN MAC Address	This field displays the MAC address of the ZyXEL Device on the WAN.
LAN MAC Address	This field displays the MAC address of the ZyXEL Device on the LAN.
Network	
WAN Status	This field displays the status of the ZyXEL Device'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 ZyXEL Device.
LAN IP Address LAN Subnet Mask	This field displays the IP address and the subnet mask of the LAN port on the ZyXEL Device.
Default Gateway	This field displays the IP address of the default gateway of the WAN port on the ZyXEL Device.
DNS	This field displays the IP address of the DNS server that the ZyXEL Device is using.
Wireless	
Wireless Service	This field displays the status of the ZyXEL Device's wireless LAN.
ESSID	This field displays the ZyXEL Device's Extended Service Set IDentity.
Wireless Channel	This field displays the channel that the ZyXEL Device is using.
Encryption	This field displays the type of data encryption that the ZyXEL Device is using. **WEP** displays if the ZyXEL Device is using WEP data encryption. **WPA** displays if ZyXEL Device is using WPA data encryption. **Disable** displays if the ZyXEL Device is not using data encryption.
Traffic	
WAN	This field displays traffic statistics for the ZyXEL Device's WAN connection.
LAN	This field displays traffic statistics for the ZyXEL Device's LAN connection.
Wireless	This field displays traffic statistics for the ZyXEL Device's wireless LAN connection.

2.7 Login Accounts

There are four system accounts that you can use to log in to the ZyXEL Device: 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".

Downloaded from www.Manualslib.com manuals search engine

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 is "supervisor".

Use the super subscriber account to test the Internet connection between the ZyXEL Device and the ISP. The ZyXEL Device 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".

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

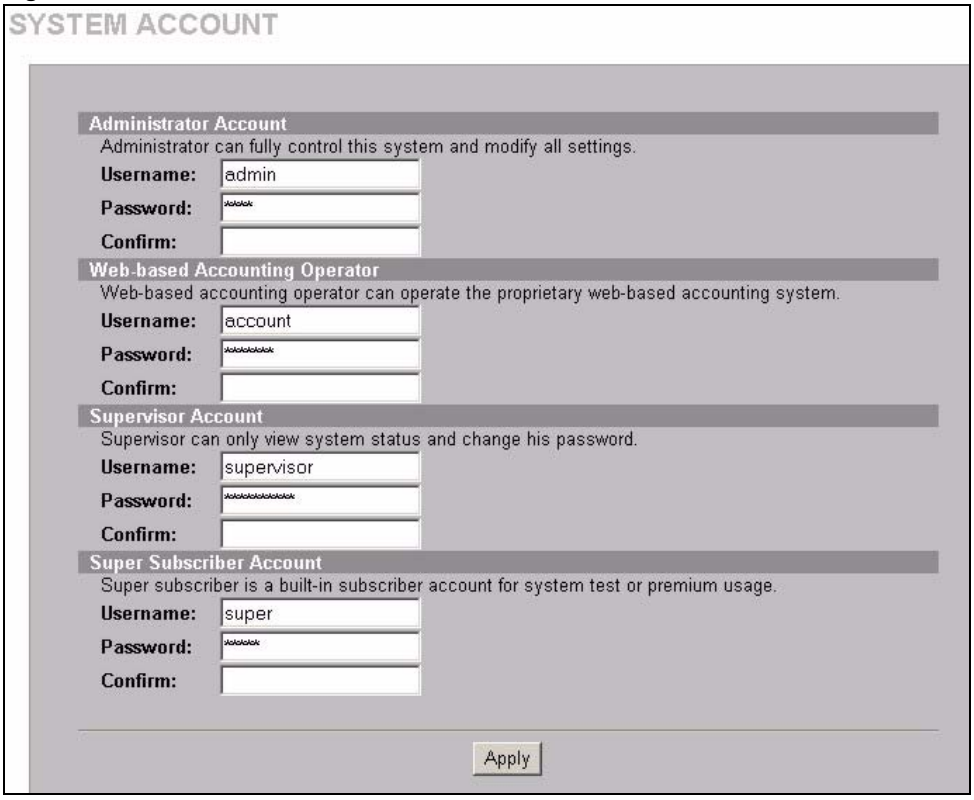
2.7.1 Changing Login Account Usernames and Passwords

Note: It is recommended you change the account passwords.

Click **SYSTEM TOOLS > SYSTEM ACCOUNT** to open the following screen.

Downloaded from www.Manualslib.com manuals search engine

Figure 8 SYSTEM TOOLS > SYSTEM ACCOUNT



Note: The account user names and passwords are case sensitive.

Table 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.

Downloaded from www.Manualslib.com manuals search engine

Table 3 SYSTEM TOOLS > SYSTEM ACCOUNT (continued)

LABEL	DESCRIPTION
Super Subscriber Account	**Note:** 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 ZyXEL Device.

2.8 Methods of Restoring Factory-Defaults

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

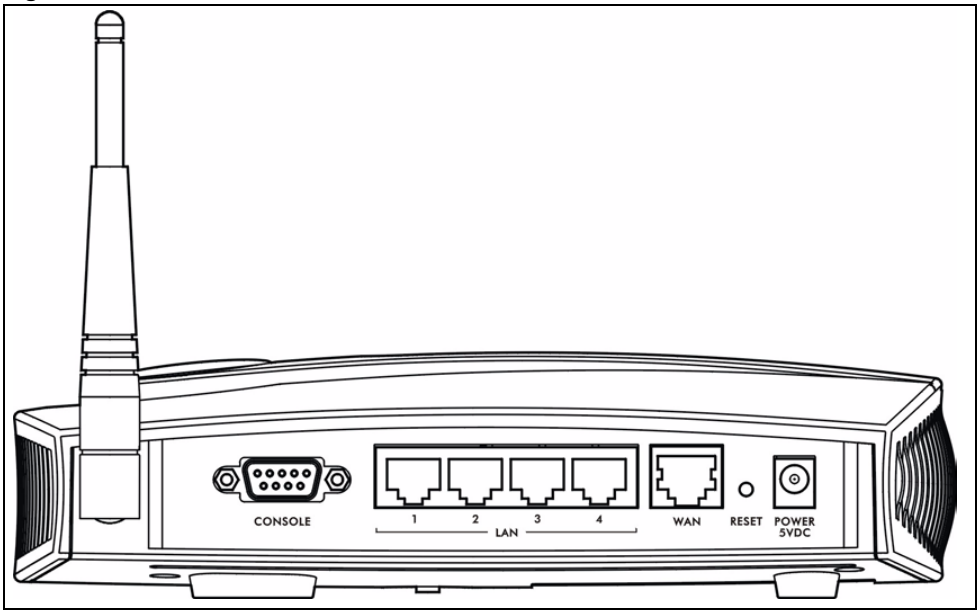
2.8.1 Using the Reset Button to Restore Factory-Defaults

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

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

Downloaded from www.Manualslib.com manuals search engine

Figure 9 Side Panel

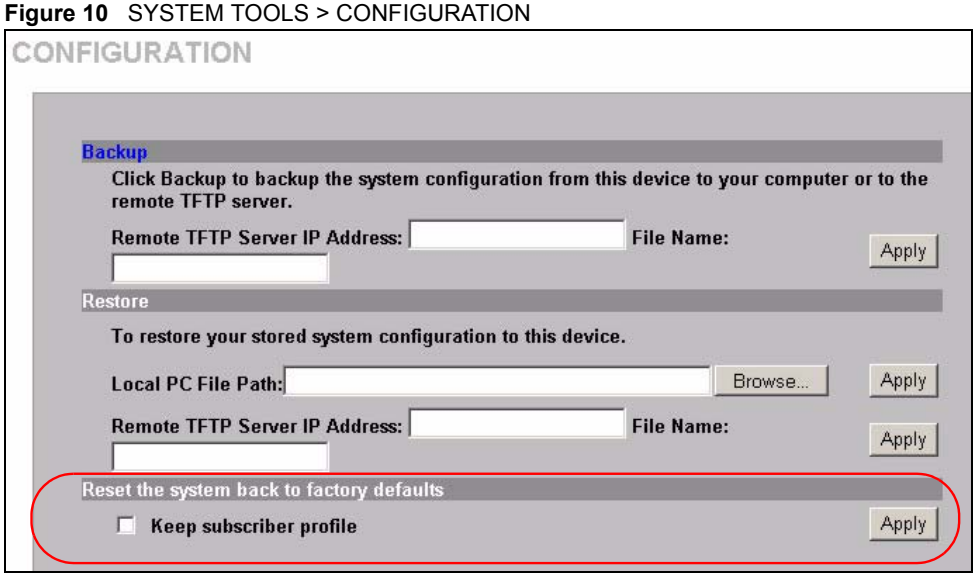


2.8.2 Using the Web Configurator to Restore Factory-Defaults

To reset the ZyXEL Device back to the factory defaults, click **SYSTEM TOOLS > CONFIGURATION** to display the screen as shown next.

Downloaded from www.Manualslib.com manuals search engine

Figure 10 SYSTEM TOOLS > CONFIGURATION



The following table describes the labels in this screen.

Table 4 SYSTEM TOOLS > CONFIGURATION

LABEL	DESCRIPTION
Reset the system back to factory defaults	
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.
Apply	Click **Apply** to reset system configuration back to the factory defaults.

2.9 Restarting the ZyXEL Device

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

Click **SYSTEM TOOLS > RESTART**. Then click **Apply**.

Downloaded from www.Manualslib.com manuals search engine

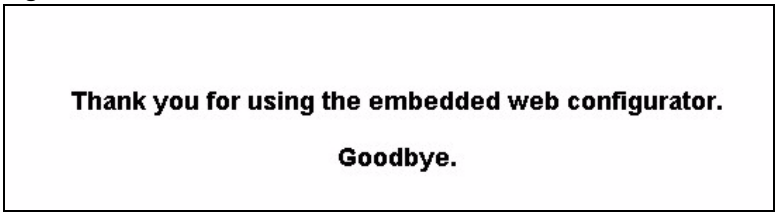
Figure 11 Restart

Note: When the ZyXEL Device 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.

2.10 Logging Out of the Web Configurator

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

Figure 12 LOGOUT



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 3
General System Setup

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

3.1 General System Setup

Use this screen to configure administrative and system-related general settings for your ZyXEL Device.

3.2 System Name

System name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

In Windows 95/98 click Start, Settings, Control Panel, Network. Click the Identification tab, note the entry for the Computer Name field and enter it as the System Name.

In Windows 2000, click Start, Settings and Control Panel and then double-click System. Click the Network Identification tab and then the Properties button. Note the entry for the Computer name field and enter it as the System Name.

In Windows XP, click Start, My Computer, View system information and then click the Computer Name tab. Note the entry in the Full computer name field and enter it as the ZyXEL Device System Name.

3.3 Domain Name

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 ZyXEL Device via DHCP.

3.4 iPnP ZyXEL Implementation

Traditionally, you must set the IP addresses and the subnet masks of a computer and the ZyXEL Device to be in the same subnet to allow the computer to access the Internet (through the ZyXEL Device). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the ZyXEL Device.

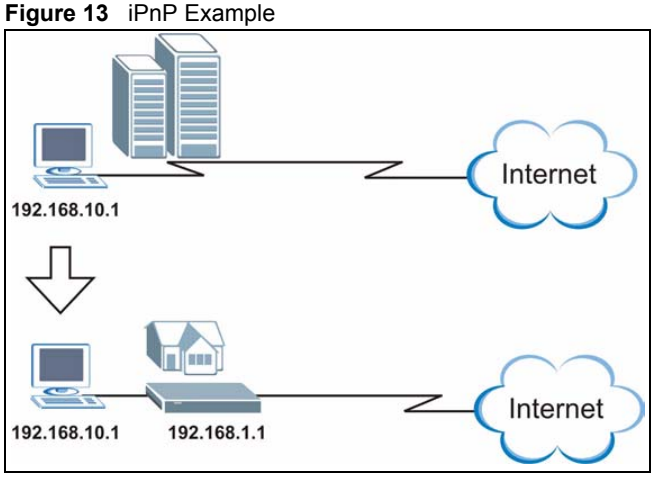
Downloaded from www.Manualslib.com manuals search engine

With the iPnP feature and NAT enabled, the ZyXEL Device allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. Modified

Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the ZyXEL Device and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a ZyXEL Device is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.

Figure 13 iPnP Example



The iPnP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the ZyXEL Device's IP address.Added

Note: You *must* enable NAT to use the iPnP feature.

3.4.1 How iPnP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the ZyXEL Device) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the ZyXEL Device.

1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.

Downloaded from www.Manualslib.com manuals search engine

2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The ZyXEL Device receives the ARP request and replies to the computer with its own MAC address.
4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the ZyXEL Device.
5. When the ZyXEL Device receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

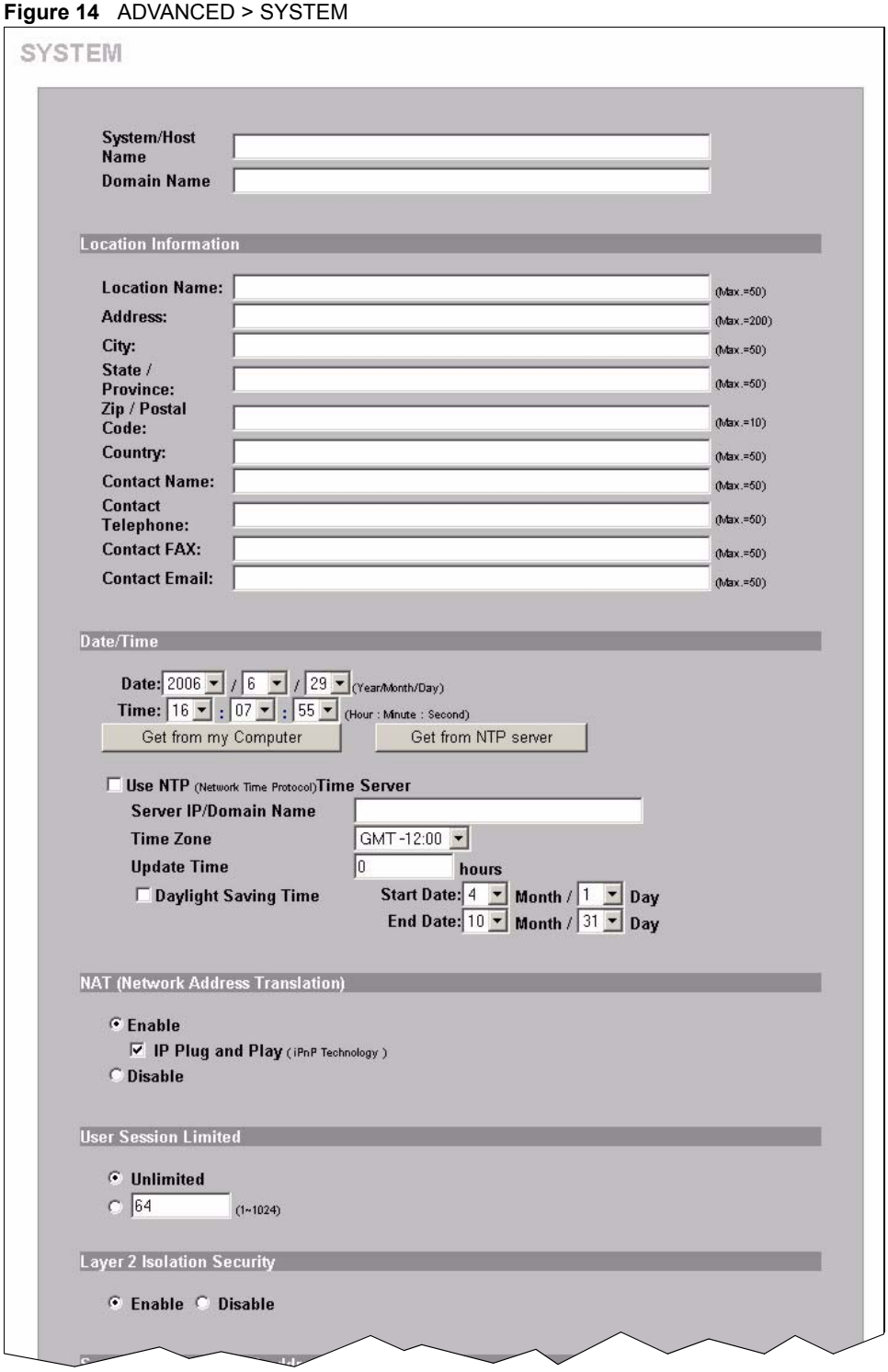
After all the routing information is updated, the computer can access the ZyXEL Device and the Internet as if it is in the same subnet as the ZyXEL Device.

3.5 General System Settings

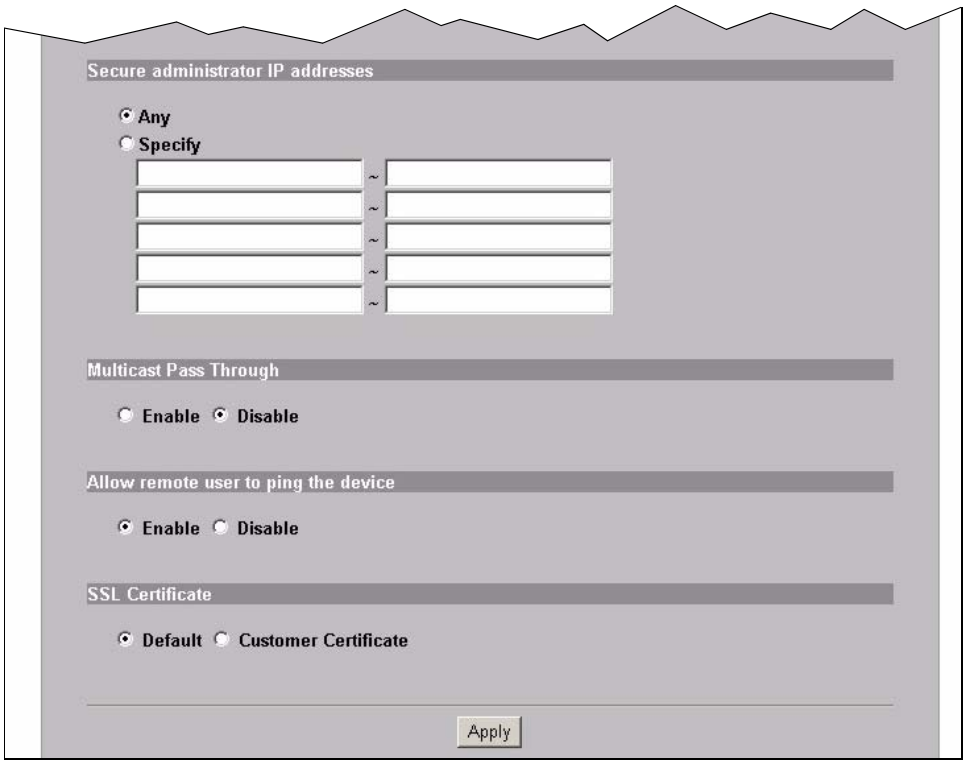
Click **ADVANCED > SYSTEM** to open this screen.

Downloaded from www.Manualslib.com manuals search engine

Figure 14 ADVANCED > SYSTEM



Downloaded from www.Manualslib.com manuals search engine



The following table describes the labels in this screen.

Table 5 ADVANCED > SYSTEM

LABEL	DESCRIPTION
System/Host 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 ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

Table 5 ADVANCED > SYSTEM (continued)

LABEL	DESCRIPTION
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 ZyXEL Device to be the same as the management computer.
Get from NTP server	Click this button to set the time and date on the ZyXEL Device to be the same as the management computer.
Use NTP (Network Time Protocol) Time Server	Select this check box to set the ZyXEL Device 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.
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 ZyXEL Device uses the NTP server to update the time and date.
Daylight Saving Time	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 Time**.
End Date	Select the month and day that your daylight-savings time ends on if you selected **Daylight Saving Time**.
NAT (Network Address Translation)	Enable NAT to have the ZyXEL Device 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)	Select this option to activate the iPnP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. When you disable the iPnP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyXEL Device's LAN IP address can connect to the ZyXEL Device or access the Internet through the ZyXEL Device.
User Session Limited	Select **Unlimited** to not place any restriction on the number of sessions that each user connected to the ZyXEL Device can use. Select the other radio button and type a number (from 1 to 1024) if you want to specify how many sessions each user connected to the ZyXEL Device can use.
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.
Secure administrator IP addresses	Select **Any** to use any computer to access the web configurator on the ZyXEL Device. 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 ZyXEL Device. The addresses can be on the LAN or the WAN.

Downloaded from www.Manualslib.com manuals search engine

Table 5 ADVANCED > SYSTEM (continued)

LABEL	DESCRIPTION
Multicast Pass Through	Select **Enable** to allow multicast traffic to pass through the ZyXEL Device. This may affect your network performance. Select **Disable** to prevent any multicast traffic from passing through the ZyXEL Device. This is the default setting.
Allow remote user to ping the device	This feature affects the security of the ZyXEL Device'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 ZyXEL Device respond to incoming Ping requests from the WAN. This is less secure since someone on the Internet can see that the ZyXEL Device is there by pinging it. Select **Disable** to have the ZyXEL Device not respond to incoming Ping requests from the WAN. This is more secure since someone on the Internet cannot see that the ZyXEL Device is there by pinging it.
SSL Certificate	Secure Socket Layer (SSL) security allows you to create secure connections between the ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

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 ZyXEL Device 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 ZyXEL Device obtains from a DHCP server on a network. A dynamic IP is not fixed; the DHCP server provides an IP address to the ZyXEL Device 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 ZyXEL Device 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 ZyXEL Device can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

Downloaded from www.Manualslib.com manuals search engine

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 on page 58); 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.*

Downloaded from www.Manualslib.com manuals search engine

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) 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.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS).

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 ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

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.

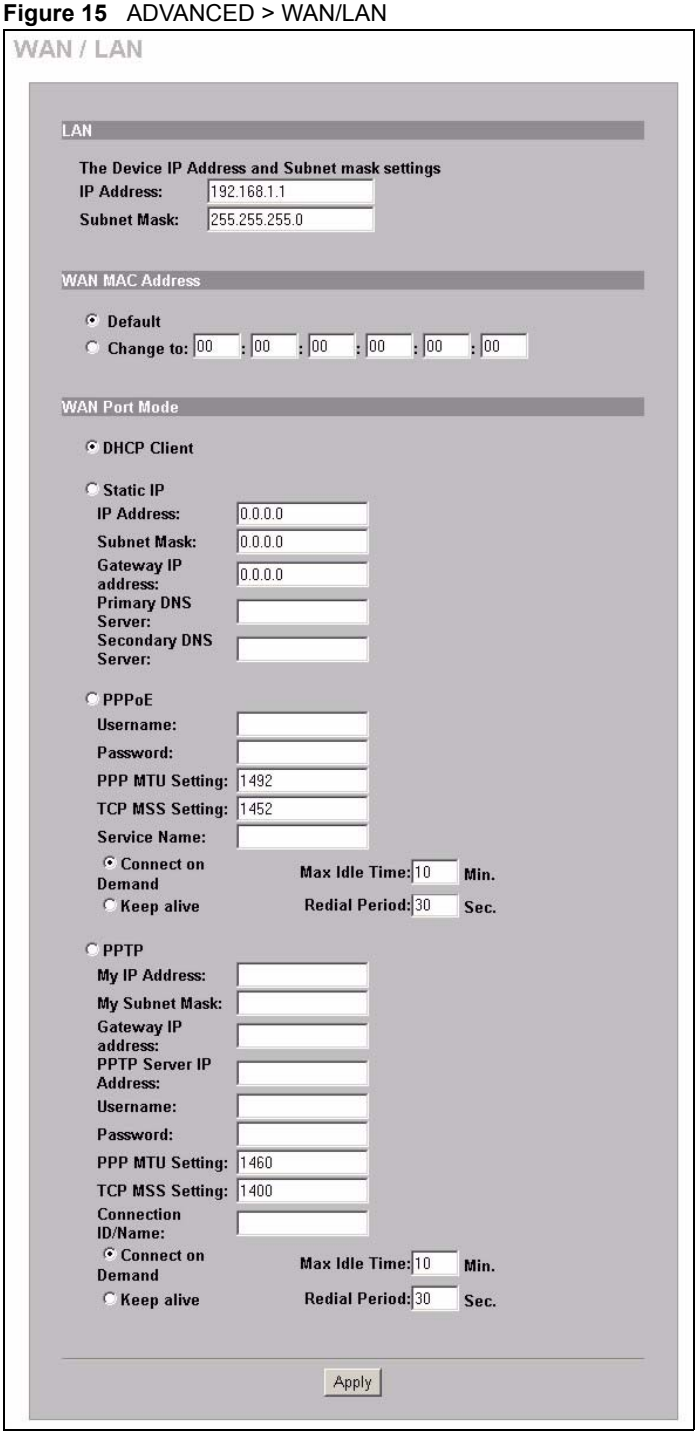
PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

4.8 Configuring the WAN and LAN Settings

To configure the WAN and LAN settings on the ZyXEL Device, click **ADVANCED > WAN/LAN** to display the screen shown next.

Downloaded from www.Manualslib.com manuals search engine

Figure 15 ADVANCED > WAN/LAN



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 6 ADVANCED > LAN/WAN

LABEL	DESCRIPTION
LAN	
IP Address	Enter the LAN IP address of the ZyXEL Device 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 ZyXEL Device to act as a DHCP client on the WAN. The ZyXEL Device 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 ZyXEL Device 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. The gateway is a router or switch on the same network segment as the ZyXEL Device. The gateway helps forward packets to their destinations. Leave this field as **0.0.0.0** if you do not know it.
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 on page 59 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.
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 ZyXEL Device will attempt to bring up the connection after the redial period.
PPTP	Select this option to activate **PPTP** support. Refer to Section 4.7 on page 60 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.

Downloaded from www.Manualslib.com manuals search engine

Table 6 ADVANCED > LAN/WAN (continued)

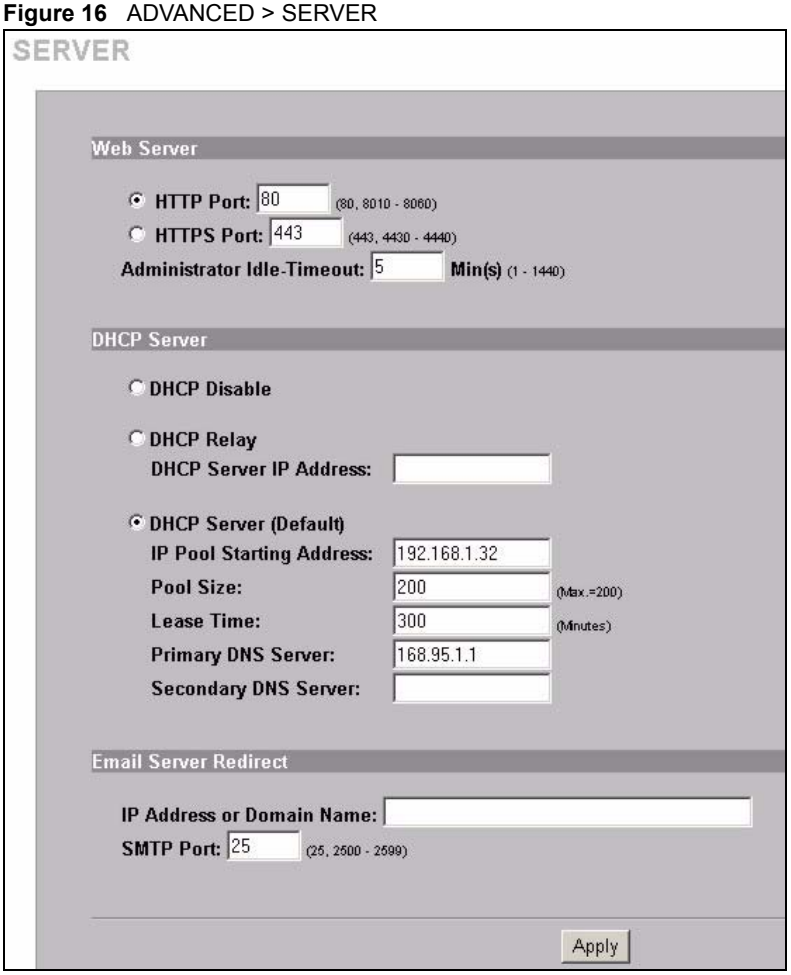
LABEL	DESCRIPTION
Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form *user@domain* where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the MTU (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 ZyXEL Device will attempt to bring up the connection after the redial period.
Apply	Click **Apply** to save the changes.

4.9 Server Configuration

Click **ADVANCED > SERVER** to display the screen as shown next. Use this screen to set the embedded web server, the LAN DHCP server and specify the e-mail server for e-mail redirection on the ZyXEL Device.

Downloaded from www.Manualslib.com manuals search engine

Figure 16 ADVANCED > SERVER



Downloaded from www.Manualslib.com manuals search engine

The following table describes the fields in this screen.

Table 7 ADVANCED > SERVER

LABEL	DESCRIPTION
Web Server	
HTTP Port	Select this radio button if you want to access the ZyXEL Device using unsecured HTTP. Specify the port number of the embedded web server on the ZyXEL Device for accessing the web configurator. The default port number is **80**. Changing the port number helps protect the ZyXEL Device'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 8010 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://192.168.1.1:8010" where 192.168.1.1 is the WAN or LAN port IP address.
HTTPS Port	Select this radio button if you want to access the ZyXEL Device using secure HTTPS. Secure Socket Layer (SSL) security allows you to create secure connections between the ZyXEL Device and the management computer(s). Refer to the *SSL (Secure Socket Layer) Security* chapter for more information. Specify the port number of the embedded web server on the ZyXEL Device for accessing the web configurator. The default port number is **443**. Changing the port number helps protect the ZyXEL Device's web configurator from hacker attacks. Enter a number between 4430 and 4440 to access the web configurator behind a NAT-enabled network. If you enter a number between 4430 and 4440, 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 "4430" as the web server port number, then you must enter "https://192.168.1.1:4430" where 192.168.1.1 is the WAN or LAN port IP address.
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 ZyXEL Device. Select this option to set the ZyXEL Device 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).
DHCP Server (Default)	Select this option to set the ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

Table 7 ADVANCED > SERVER (continued)

LABEL	DESCRIPTION
DHCP Pool Size	This field specifies the size or count of the IP address pool. Enter a number not greater than 1024.
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. **Note:** 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 ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 5
Authentication

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

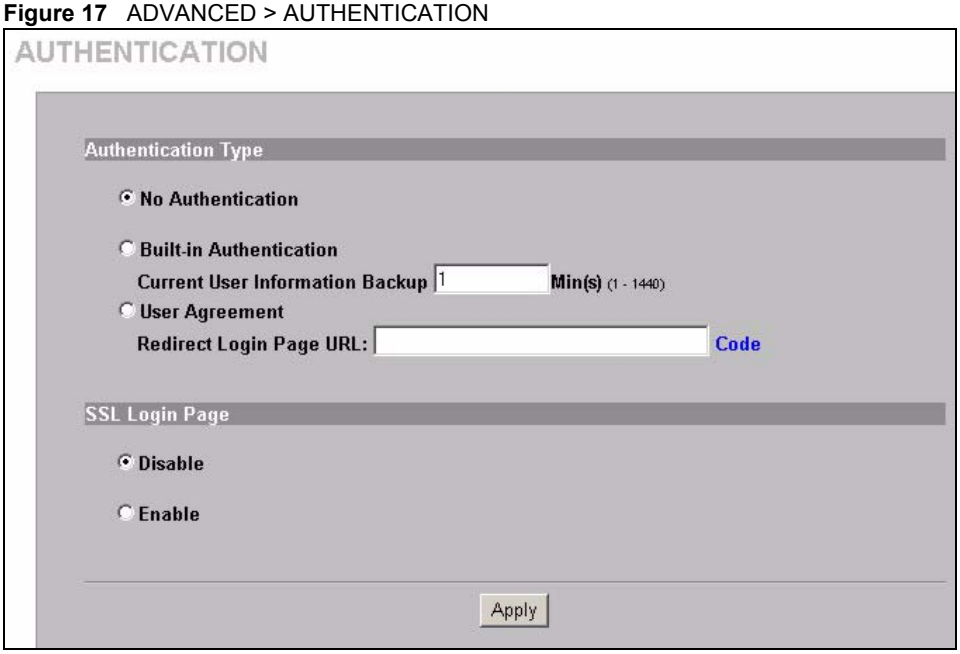
5.1 About the Built-in Authentication

You can use the built-in subscriber database to manage the subscribers. The ZyXEL Device 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 > AUTHENTICATION** to display the screen as shown next.

Figure 17 ADVANCED > AUTHENTICATION



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 8 ADVANCED > 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. **Note:** 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 ZyXEL Device 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 the user agreement page to send the subscribers' agreement or disagreement to the ZyXEL Device. Use up to 350 ASCII characters.
SSL Login Page	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 ZyXEL Device. 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.

Click **ADVANCED > AUTHENTICATION > Code** to display the HTML source code of a default sample page (shown next). The user agreement page must include the HTML source code in the default sample page in order for the user agreement page to send the subscribers' agreement or disagreement to the ZyXEL Device.

Downloaded from www.Manualslib.com manuals search engine

Figure 18 ADVANCED > AUTHENTICATION > Code

Redirect Page Sample Code

```
<html>
<body>
<center>
<table width="100%" border="0">
<tr>
<td align="right" width="45%">
<form method="post" action="http://1.1.1.1/agree.cgi" name="agree">
<input type="submit" name="agree" value="Agree">
</form>
</td>
<td width="10%"> </td>
<td width="45%">
<form method="post" action="http://1.1.1.1/disagree.cgi"
name="disagree">
<input type="submit" name="disagree" value="Do not agree">
</form>
</td>
</tr>
</table>
</center>
</body>
</html>
```

Close

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 6
RADIUS

This chapter shows you how to configure the ZyXEL Device to use an external RADIUS server.

6.1 About RADIUS

You can use an external RADIUS (Remote Authentication Dial-In User Service) server to authenticate the subscriber connections and keep track of accounting information.

RADIUS is based on a client-sever model that supports authentication, authorization and accounting. This system is the client and the server is the external RADIUS server.

RADIUS is a simple package exchange in which the ZyXEL Device acts as a message relay between the subscribers and the RADIUS server to establish a connection. When you enable RADIUS authentication, the ZyXEL Device uses RADIUS protocol (RFC 2865, 2866) to send subscriber authentication information to the external RADIUS server.

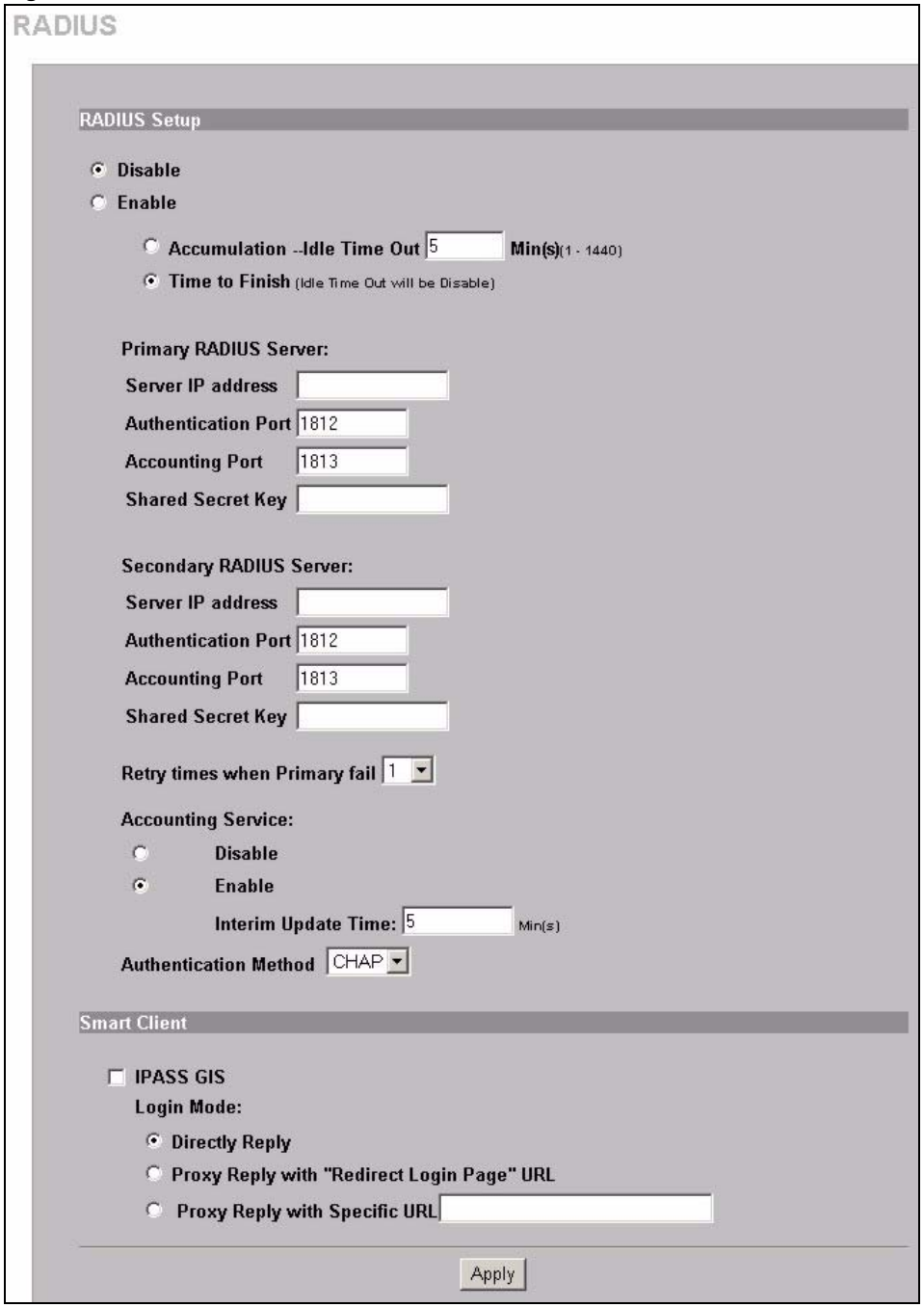
When you use an external RADIUS server for accounting, you can use either accumulation or time to finish accounting. See Chapter 7 on page 75 for information on accumulation and time to finish accounting.

6.2 RADIUS Settings

Click **ADVANCED > RADIUS** to display the screen as shown next.

Downloaded from www.Manualslib.com manuals search engine

Figure 19 ADVANCED > RADIUS



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 9 ADVANCED > RADIUS

LABEL	DESCRIPTION
RADIUS Setup	Select **Disable** if you will not use an external RADIUS server to authenticate subscribers. Select **Enable** to use an external RADIUS server to authenticate subscribers. You may also use an external RADIUS server to perform accounting for the subscriber accounts. **Note:** Disabling authentication in the AUTHENTICATION screen also disables authentication via an external RADIUS server, regardless of what you set here.
Accumulation	Select this option to allow each subscriber multiple re-login until the time allocated is used up. This applies to subscribers that are authenticated by the RADIUS server; the setting in the **BILLING** screen applies to subscribers that are authenticated by the built-in authentication. You must also enable the accounting service below.
Idle Time Out	The ZyXEL Device 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.
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. This applies to subscribers that are authenticated by the RADIUS server; the setting in the **BILLING** screen applies to subscribers that are authenticated by the built-in authentication. You must also enable the accounting service below.
Primary RADIUS Server	
Server IP address	Enter the IP address of the RADIUS server in dotted decimal notation.
Authentication Port	Enter the port number that the RADIUS server uses for authentication. You only need to change this value from the default if your network administrator gave you a specific port number to use. The allowed numbers are from 0 to 65535.
Accounting Port	Enter the port number that the RADIUS server uses for accounting. You only need to change this value from the default if your network administrator gave you a specific port number to use. The allowed numbers are from 0 to 65535.
Shared Secret Key	Enter a password (up to 64 characters) as the key to be shared between the RADIUS server and the ZyXEL Device. The key is not sent over the network. This key must be the same on the RADIUS server and the ZyXEL Device.
Secondary RADIUS Server	
Server IP address	Enter the IP address of the RADIUS server in dotted decimal notation.

Downloaded from www.Manualslib.com manuals search engine

Table 9 ADVANCED > RADIUS (continued)

LABEL	DESCRIPTION
Authentication Port	Enter the port number that the RADIUS server uses for authentication. You only need to change this value from the default if your network administrator gave you a specific port number to use. The allowed numbers are from 0 to 65535.
Accounting Port	Enter the port number that the RADIUS server uses for accounting. You only need to change this value from the default if your network administrator gave you a specific port number to use. The allowed numbers are from 0 to 65535.
Shared Secret Key	Enter a password (up to 64 characters) as the key to be shared between the RADIUS server and the ZyXEL Device. The key is not sent over the network. This key must be the same on the RADIUS server and the ZyXEL Device.
Retry times when Primary fail	At times the ZyXEL Device may not be able to use the primary RADIUS server. Select the number of times the ZyXEL Device should reattempt to use the primary RADIUS server before attempting to use the secondary RADIUS server. This also sets how many times the ZyXEL Device will attempt to use the secondary RADIUS server. For example, you set this field to 3. If the ZyXEL Device does not get a response from the primary RADIUS server, it tries again up to three times. If there is no response, the ZyXEL Device tries the secondary RADIUS server up to three times. If there is also no response from the secondary RADIUS server, the ZyXEL Device stops attempting to authenticate the subscriber. The subscriber will see a message that says the RADIUS server was not found.
Accounting Service	Select **Disable** if you will not use an external RADIUS server to perform accounting for the wireless client accounts. Select **Enable** to use an external RADIUS server to perform accounting for the wireless client accounts.
Interim Update Time	Specify the time interval for how often the ZyXEL Device is to send a subscriber status update to the RADIUS server.
Authentication Method	Enter the authentication protocol that the RADIUS server uses. PAP (Password Authentication Protocol) requires users to enter a password before accessing a secure system. The user's name and password are sent over the wire to a server where they are compared with a database of user account names and passwords. CHAP (Challenge Handshake Authentication Protocol) avoids sending passwords over the wire by using a challenge/response technique.
IPASS GIS	The iPass company provides connectivity services for mobile Internet users. Select this check box to have the ZyXEL Device use the iPass Generic Interface Specification (GIS) method to authenticate iPass clients. Your external RADIUS servers must be Wi-Fi based Wireless Internet Service Provider roaming (WISPr) compliant in order to authenticate iPass clients.
Login Mode	When using iPass GIS, your ISP will provide you with login mode information. Select **Directly Reply**, **Proxy Reply with "Redirect Login Page" URL** or **Proxy Reply with Specific URL** (and enter a URL of up to 350 ASCII characters in the field provided). The login mode information for the iPass GIS connection. (Provided by your ISP).
Apply	Click **Apply** to save the changes.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 7
Billing

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

7.1 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.

7.1.1 Accumulation Accounting Method

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

7.1.2 Time-to-finish Accounting Method

The time-to-finish accounting method is good for one-time logins. Once a subscriber logs in, the ZyXEL Device 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.

7.2 Billing Settings

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

Downloaded from www.Manualslib.com manuals search engine

Figure 20 ADVANCED > BILLING

BILLING

Pre-Paid
Enable Credit Card Service
Time to Finish
Accumulation
Idle Time Out 5 Min(s) (1 - 1440)

Post-Paid
Idle Time Out 5 Min(s) (1 - 1440)

Billing Profile
Currency: $ (Number of decimals places: 2 .(Dot))
Tax Percentage: 5 %

No	Active	Name (max. 12 characters)	Account Usage Time		Charge
1	☑	30 minutes	30	minutes	1.00
2	☑	1 hour	1	hours	2.00
3	☑	2 hours	2	hours	3.00
4	☐	3 hours	3	hours	4.00
5	☐	5 hours	5	hours	5.00
6	☐	10 hours	10	hours	6.00
7	☐	1 day	1	days	10.00
8	☐	2 days	2	days	20.00
9	☐	7 days	7	days	50.00
10	☐	30 days	30	days	200.00

Apply

The following table describes the labels in this screen.

Downloaded from www.Manualslib.com manuals search engine

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

Table 10 ADVANCED > 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. **Note:** You must also configure your credit card service information in the **ADVANCED > BILLING** screen if you want to allow the subscribers to use credit cards to purchase Internet usage time.
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 ZyXEL Device 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. **Note:** You must use an optional keypad with the three-button printer in order to use the post-paid function.
Idle Time Out	The ZyXEL Device 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. You can also select whether you would like to use a period (.) or a comma (,) for the decimal point.
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.

Downloaded from www.Manualslib.com manuals search engine

Table 10 ADVANCED > BILLING (continued)

LABEL	DESCRIPTION
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.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 8
Accounting

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

8.1 About Subscriber Accounts

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

8.2 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 a 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.

8.2.1 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.

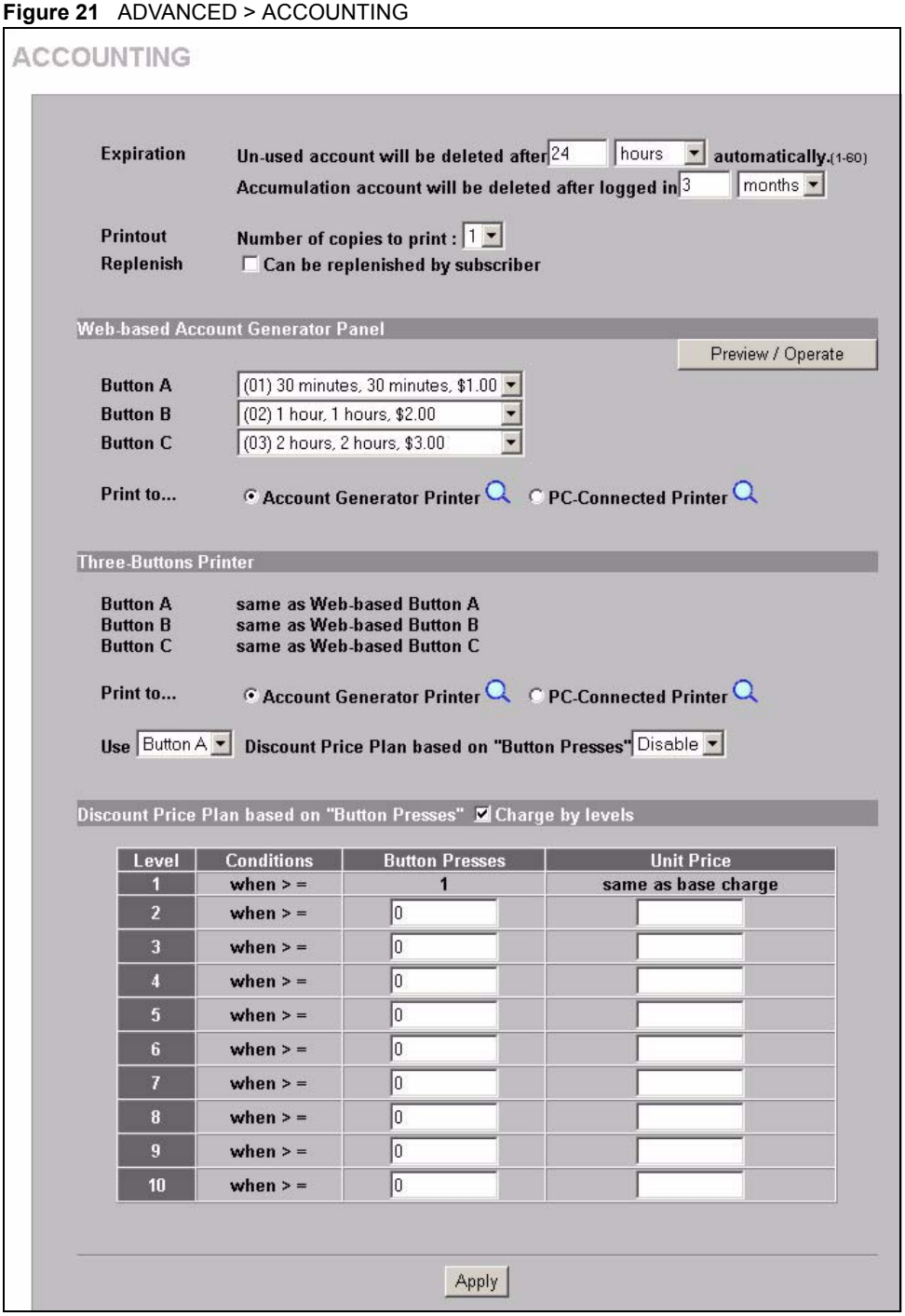
See Section 8.3.1 on page 82 for an example of the charge by levels accounting function.

8.3 Accounting Settings

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

Downloaded from www.Manualslib.com manuals search engine

Figure 21 ADVANCED > ACCOUNTING



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 11 ADVANCED > ACCOUNTING

LABEL	DESCRIPTION
Expiration	
Un-used account will be deleted after ~ automatically	Enter the number and select a time unit from the drop-down list box to specify how long to wait before the ZyXEL Device deletes an account that has not been used. 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 ZyXEL Device 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 23 on page 83).
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 ZyXEL Device via Ethernet. Select **PC-Connected Printer** if you want to print the account information using a printer connected to a network computer. Click the magnifying glass icon to display a print preview.
Three-Buttons Printer	Use this section with a three-button statement 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 ZyXEL Device via Ethernet. Select **PC-Connected Printer** if you want to print the account information using a printer connected to a network computer. Click the magnifying glass 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"	

Downloaded from www.Manualslib.com manuals search engine

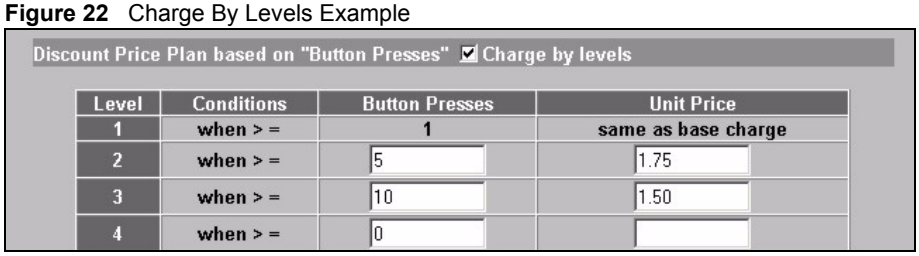
Table 11 ADVANCED > ACCOUNTING (continued)

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 ZyXEL Device.

8.3.1 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 22 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 ZyXEL Device would charge as follows:

Table 12 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)

Downloaded from www.Manualslib.com manuals search engine

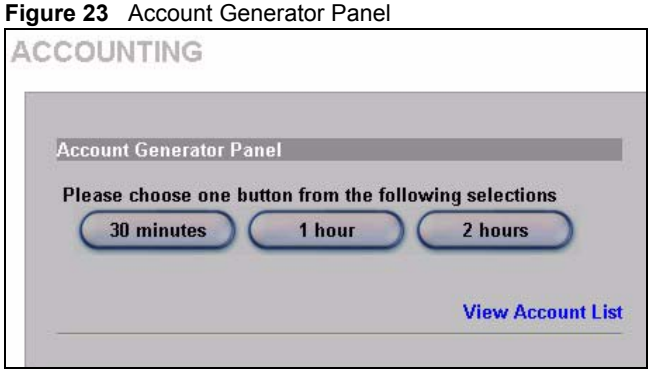
8.4 Creating Accounts

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

8.4.1 Creating Accounts in the Web Configurator

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

Figure 23 Account Generator Panel



Note: These button settings also apply to the buttons on an exclusive printer.

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

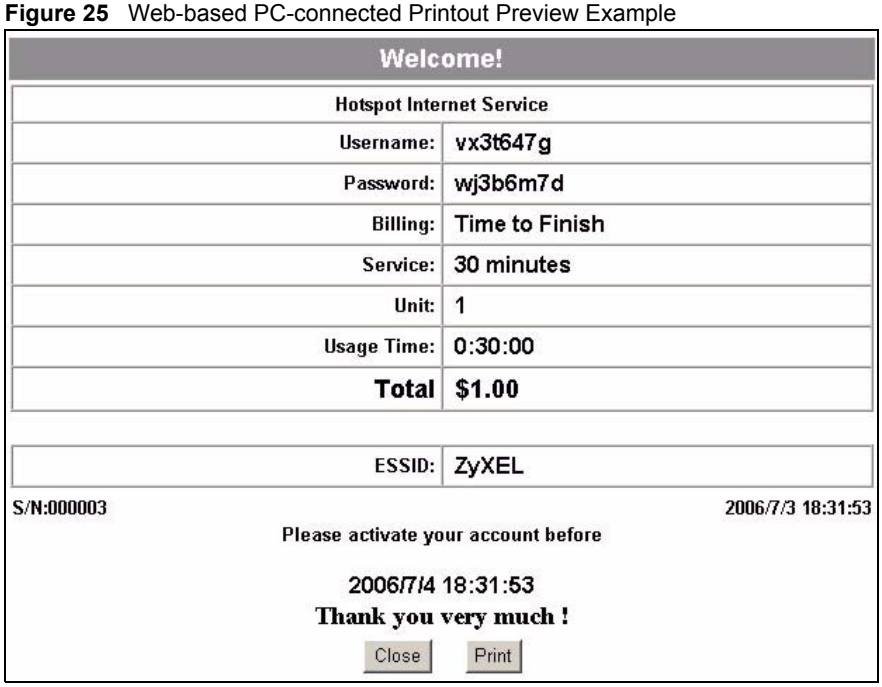
The following figure shows an example. Close this window when you are finished viewing it.

Downloaded from www.Manualslib.com manuals search engine

Figure 24 Web-based Account Generator Printout Preview Example

Downloaded from www.Manualslib.com manuals search engine

Figure 25 Web-based PC-connected Printout Preview Example



Welcome!	
Hotspot Internet Service	
Username:	vx3t647g
Password:	wj3b6m7d
Billing:	Time to Finish
Service:	30 minutes
Unit:	1
Usage Time:	0:30:00
Total	**$1.00**

ESSID:	ZyXEL

S/N:000003 2006/7/3 18:31:53

Please activate your account before

2006/7/4 18:31:53

Thank you very much !

Close Print

8.4.2 Using an 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.

1. Make sure that the printer is connected to the appropriate power and the ZyXEL Device, and that there is printing paper in the statement printer. Refer to the printer's User's Guide for details.
2. Press the button on the statement printer. The ZyXEL Device generates a dynamic account and the printer prints the subscriber's statement. Refer to Figure 24 on page 84 for a printout example.

Refer to Chapter 8 on page 79 to configure the printout page.

8.5 Viewing the Account List

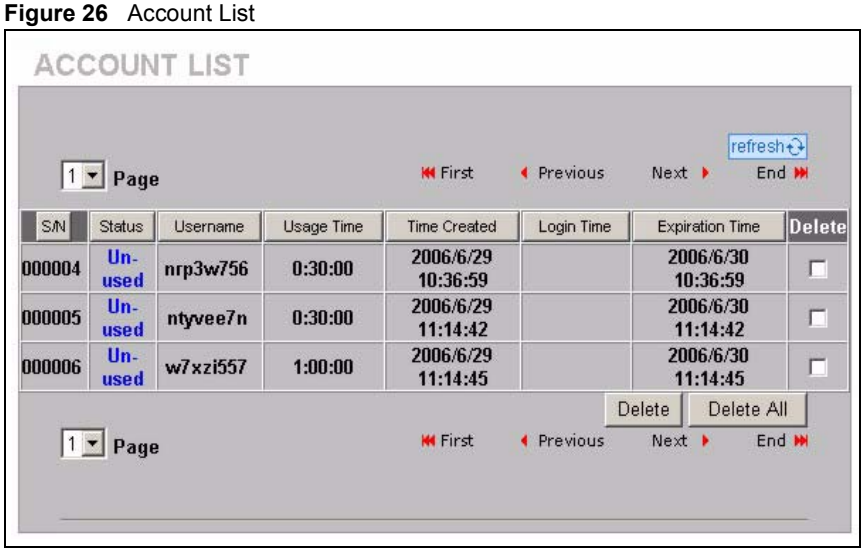
Do one of the following to view the account list.

From the **Account Generator Panel** screen, (refer to Figure 23 on page 83) click **View Account List**.

From the **SYSTEM STATUS** sub-menus, click **ACCOUNT LIST**.

Downloaded from www.Manualslib.com manuals search engine

Figure 26 Account List



The following table describes the labels in this screen.

Table 13 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.
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** check box(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.

Downloaded from www.Manualslib.com manuals search engine

Table 13 Account List (continued)

LABEL	DESCRIPTION
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 appendices for more information on logging in as a subscriber.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 9
Credit Card

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

9.1 About the Credit Card Screen

The ZyXEL Device 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) or WorldPay before you can configure the ZyXEL Device to handle credit card transactions. Call 1-866-437-0476 for an Authorize.Net account.

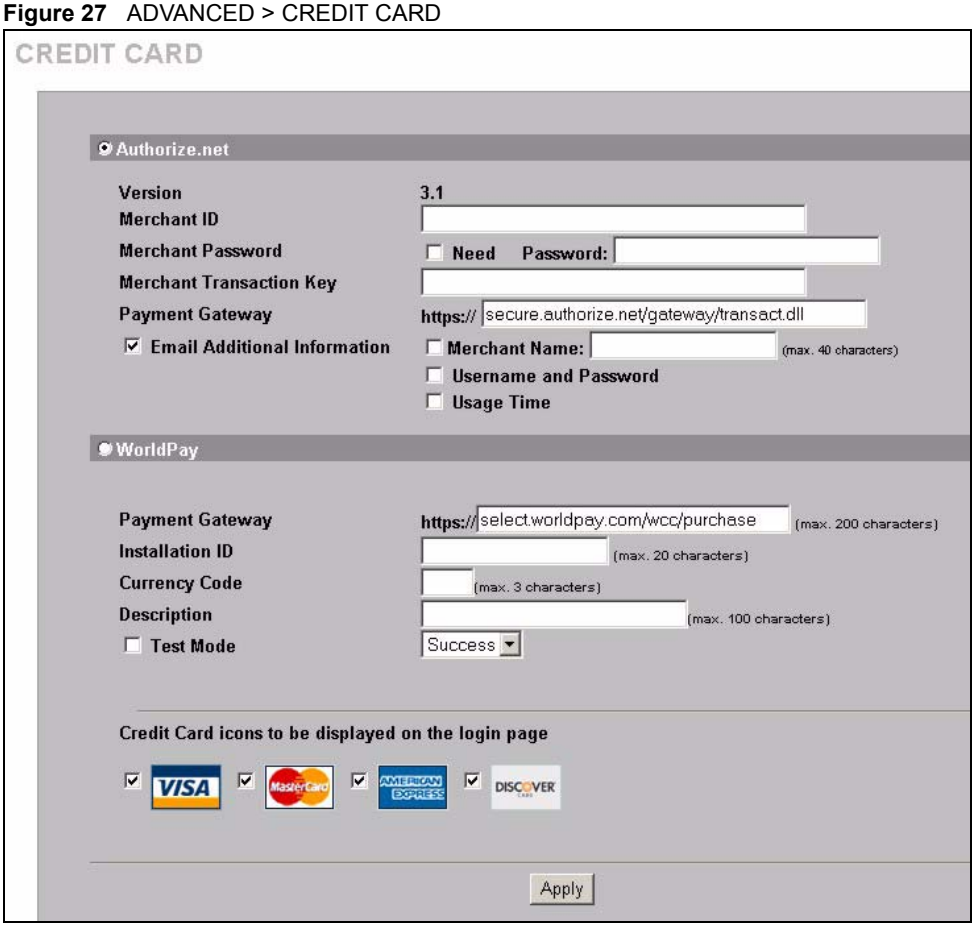
9.2 Credit Card Settings

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

Note: You also have to enable credit card services in the **ADVANCED > BILLING** screen if you want to allow the subscribers to use credit cards to purchase Internet usage time.

Downloaded from www.Manualslib.com manuals search engine

Figure 27 ADVANCED > CREDIT CARD



The following table describes the labels in this screen.

Table 14 ADVANCED > CREDIT CARD

LABEL	DESCRIPTION
Authorize.net	Select this radio button if you use Authorize.net to authorize credit card payments.
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 Password Need	Select this if you have to provide a password to Authorize.net.
Password	Enter the password you have to provide to 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.
Payment Gateway	Enter the address of the Authorize.net gateway.
Email Additional Information	Select this check box to have the ZyXEL Device e-mail the subscriber the information that you specify in the following fields.

Downloaded from www.Manualslib.com manuals search engine

Table 14 ADVANCED > CREDIT CARD (continued)

LABEL	DESCRIPTION
Merchant Name	Select this check box to have the ZyXEL Device 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 ZyXEL Device e-mail the subscriber the subscriber user name and password.
Usage Time	Select this check box to have the ZyXEL Device e-mail the subscriber the amount of usage time purchased.
WorldPay	Select this radio button if you use WorldPay to authorize credit card payments.
Payment Gateway	Enter the address of the WorldPay gateway provided to you by WorldPay after applying for your WorldPay account. The default value is "https://select.worldpay.com/wcc/purchase".
Installation ID	Enter the installation ID provided to you by WorldPay after successfully applying for your WorldPay account.
Currency Code	Enter the currency in which payments are made. The available currencies depend on your agreement with WorldPay.
Description	Enter the description of each purchase. This description appears on the customer's receipt.
Test Mode	Check this box if you want to evaluate the way WorldPay is used without actually transferring funds. There are two test modes, **Success** and **Fail**. In **Success** test mode, transactions are submitted as if the bank authorized the transaction. In **Fail** test mode, transactions are submitted as if the bank declined authorization.
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 ZyXEL Device to display on the subscriber login page.
Apply	Click **Apply** to save your settings to the ZyXEL Device.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 10
Keypad

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

10.1 About the Keypad

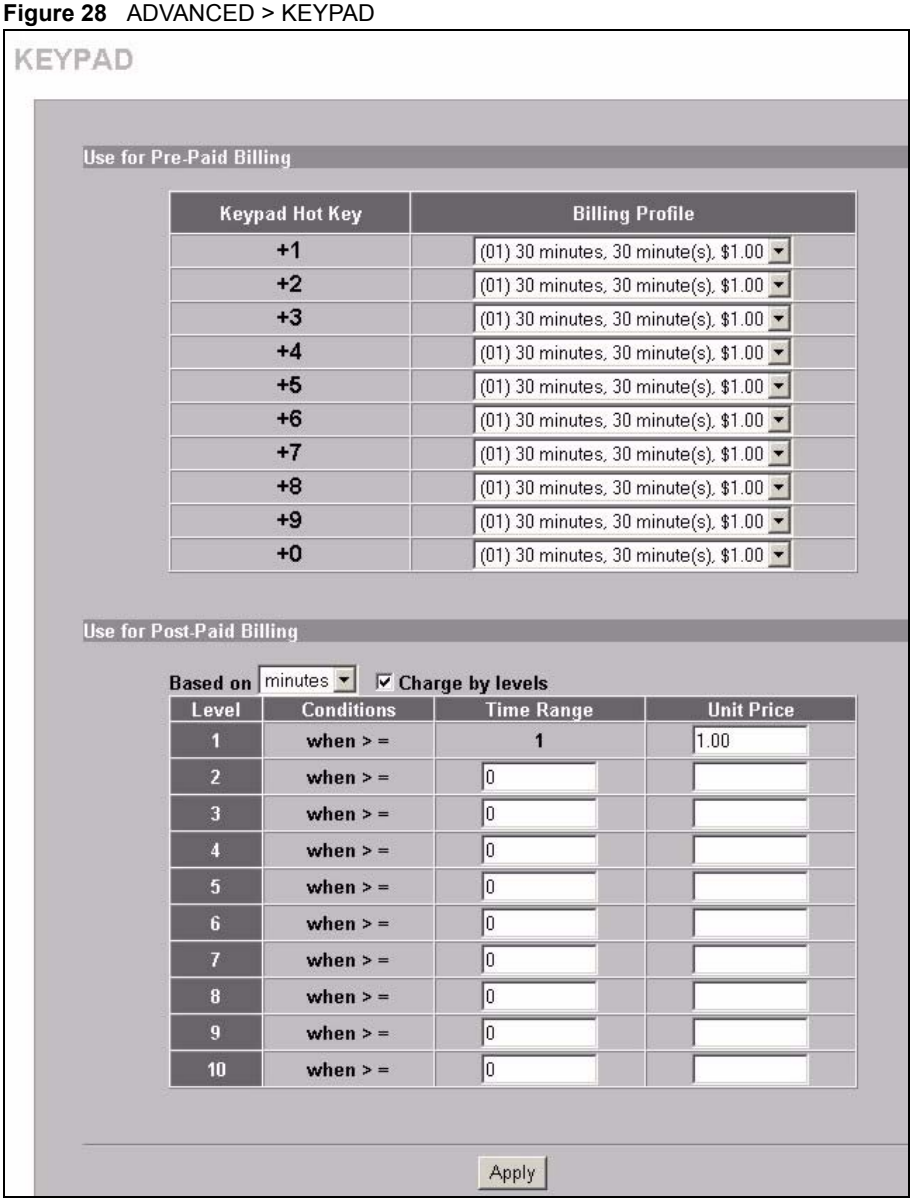
You can use an optional PS/2 numeric keypad with an exclusive printer. Use this screen to define functions for the keys.

10.2 Keypad Settings

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

Downloaded from www.Manualslib.com manuals search engine

Figure 28 ADVANCED > KEYPAD



The following table describes the labels in this screen.

Table 15 ADVANCED > 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.

Downloaded from www.Manualslib.com manuals search engine

Table 15 ADVANCED > KEYPAD (continued)

LABEL	DESCRIPTION
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.

10.3 Keypad Configuration Examples

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

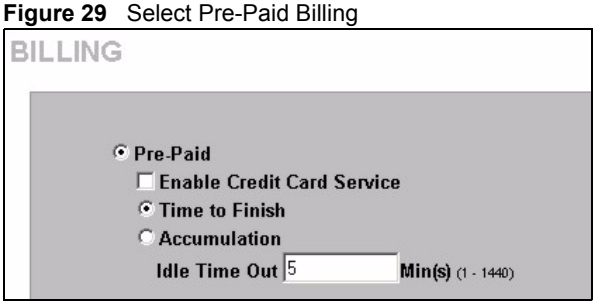
10.3.1 Keypad with Pre-Paid Billing Example

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

1 Click **ADVANCED > BILLING**.

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

Figure 29 Select Pre-Paid Billing

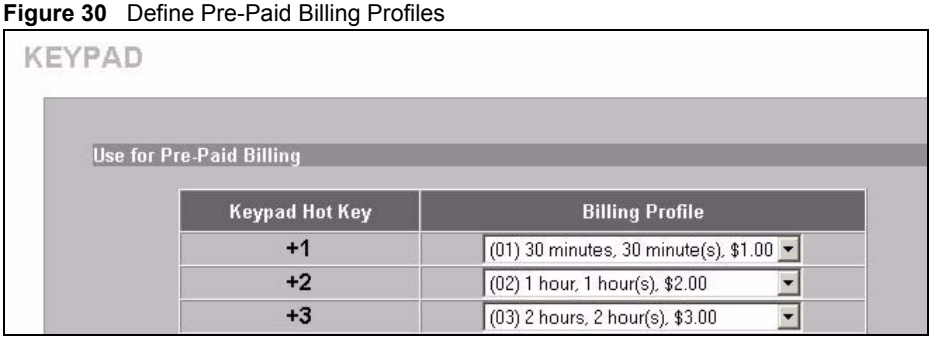


3 Click **ADVANCED > KEYPAD**.

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

Downloaded from www.Manualslib.com manuals search engine

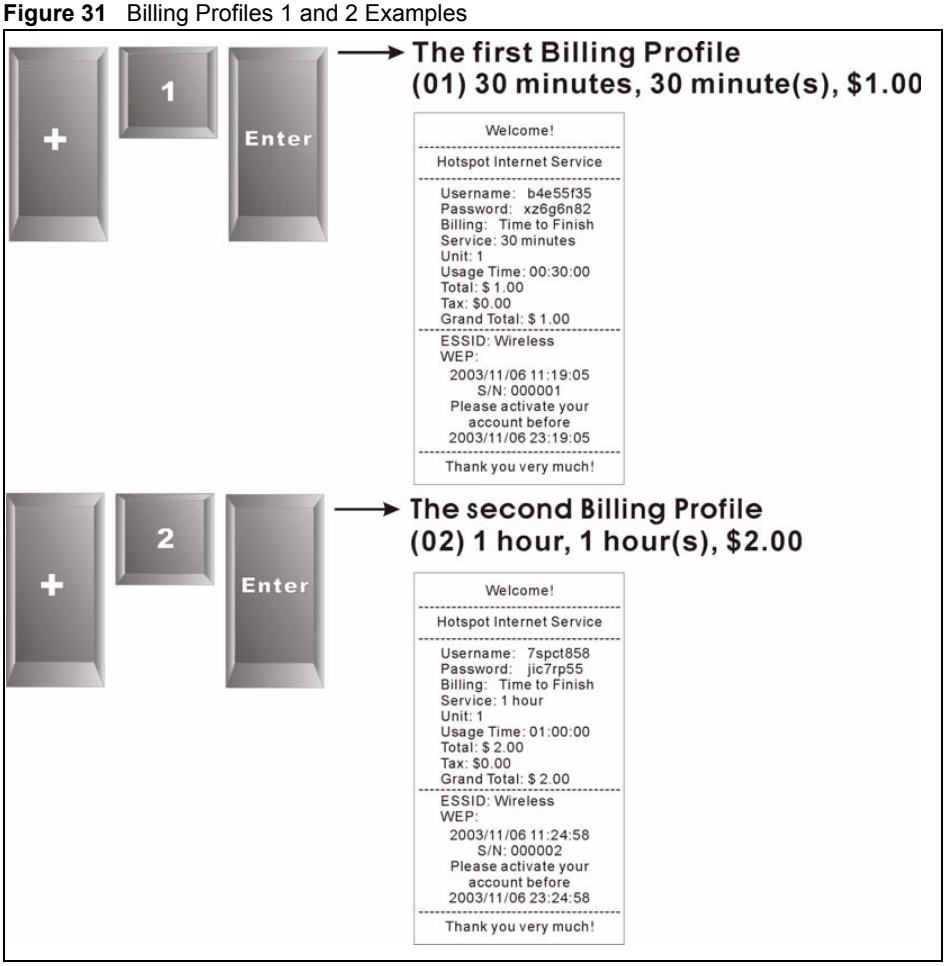
Figure 30 Define Pre-Paid Billing Profiles



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.

Downloaded from www.Manualslib.com manuals search engine

Figure 31 Billing Profiles 1 and 2 Examples



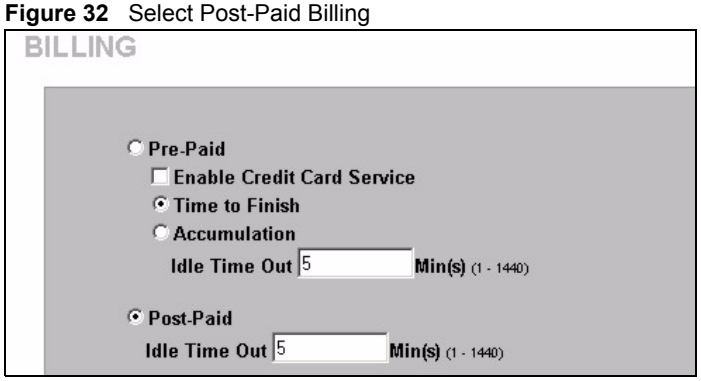
10.3.2 Keypad with Post-Paid Billing Example

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

1. Click **ADVANCED > BILLING**.
2. Select **Post-Paid** and click **Apply**.

Downloaded from www.Manualslib.com manuals search engine

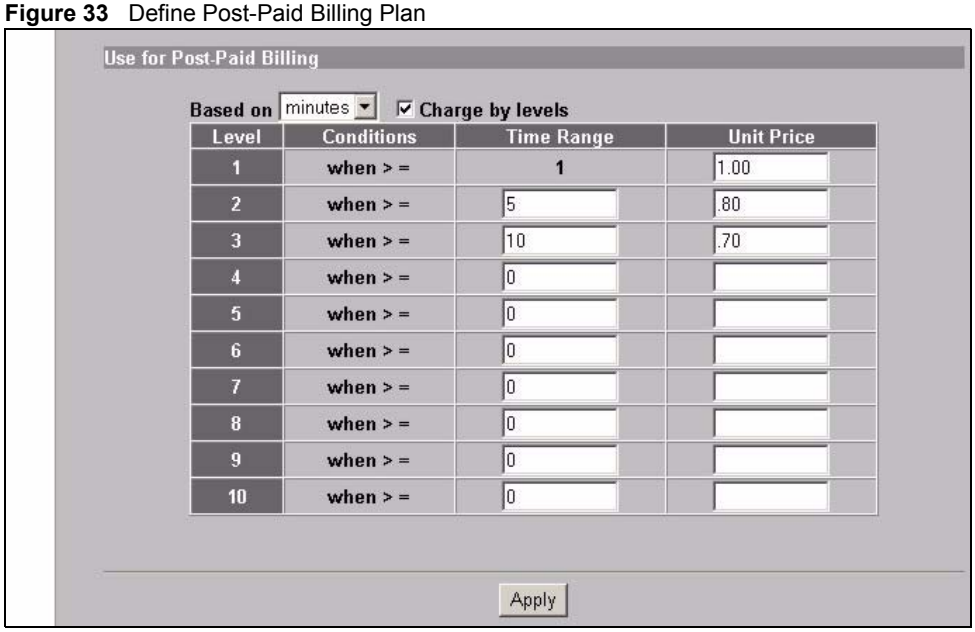
Figure 32 Select Post-Paid Billing



3 Click **ADVANCED > KEYPAD**.

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

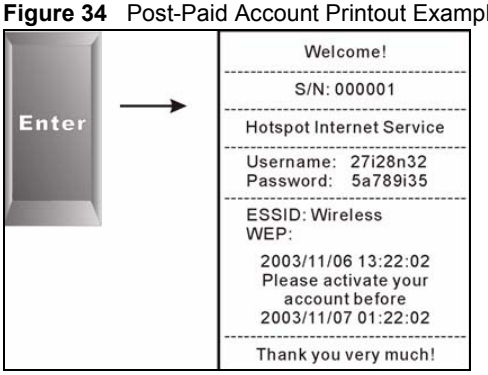
Figure 33 Define Post-Paid Billing Plan



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.

Downloaded from www.Manualslib.com manuals search engine

Figure 34 Post-Paid Account Printout Example



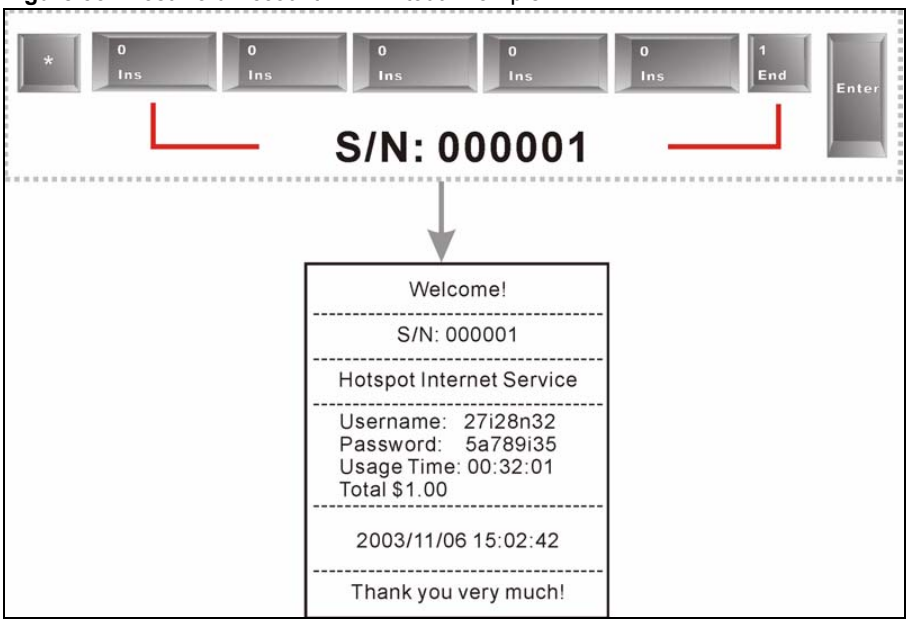
6 When a subscriber is done using the Internet service, press the following to print a bill.

a *

b Serial number

c [ENTER]

Figure 35 Post-Paid Account Bill Printout Example



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 11
Customization

This chapter shows you how to customize the subscriber interface.

11.1 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.

11.2 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).

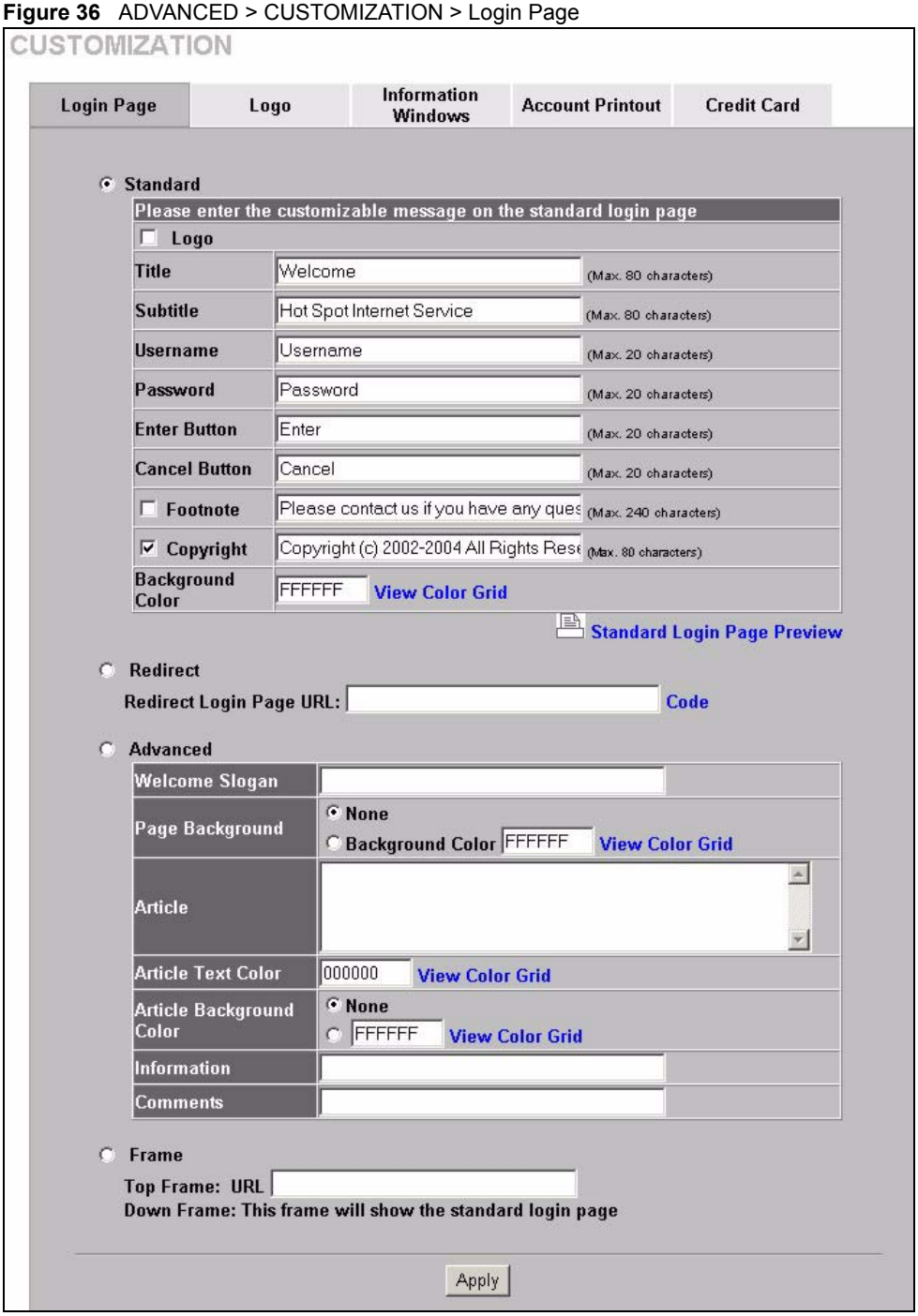
The ZyXEL Device provides different formats in which you can customize the login screen: Standard, Redirect, Advanced and Frame.

11.3 Customizing the Subscriber Login Screen

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

Downloaded from www.Manualslib.com manuals search engine

Figure 36 ADVANCED > CUSTOMIZATION > Login Page

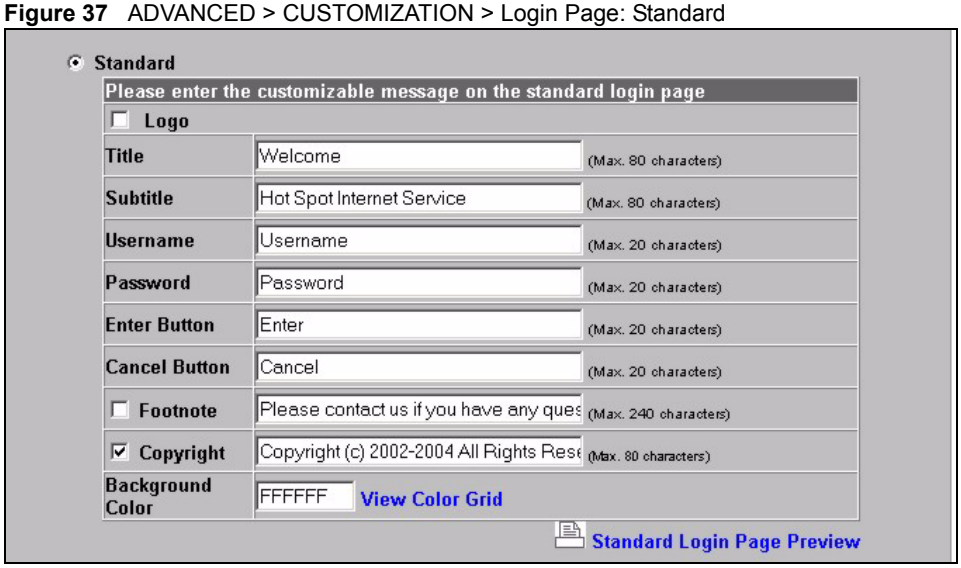


11.3.1 Standard Subscriber Login Screen

Downloaded from www.Manualslib.com manuals search engine

The standard subscriber login screen is the ZyXEL Device's pre-configured, default simple login screen. In **ADVANCED > CUSTOMIZATION > Login Page**, select **Standard**.

Figure 37 ADVANCED > CUSTOMIZATION > Login Page: Standard



The following table describes the labels in this screen.

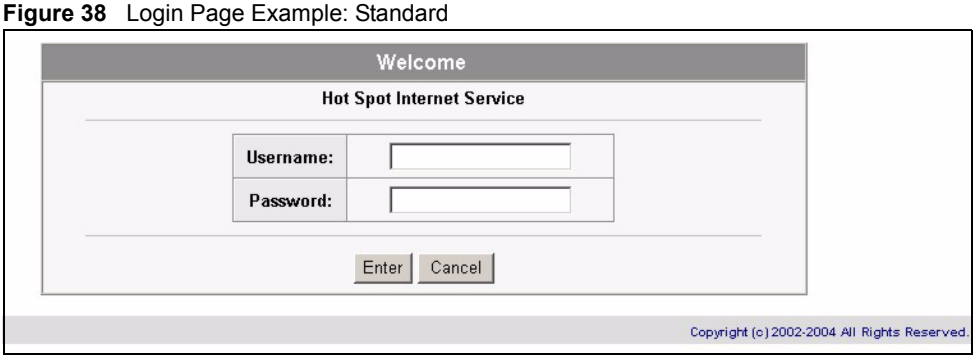
Table 16 ADVANCED > CUSTOMIZATION > Login Page: Standard

LABEL	DESCRIPTION
Logo	Select this check box to display your logo on the subscriber login screen. See Section 11.4 on page 109 for how to upload a logo file.
Title	Enter the title name (up to 80 characters) on the subscriber login page.
Subtitle	Enter the subtitle name (up to 80 characters) on the subscriber login screen.
Username	Enter the name of the **Username** field on the subscriber login screen.
Password	Enter the name of the **Password** field on the subscriber login screen.
Enter Button	Enter the name for the **Enter** button on the subscriber login screen.
Cancel Button	Enter the name for the **Cancel** button on the subscriber login screen.
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.

Downloaded from www.Manualslib.com manuals search engine

Figure 38 Login Page Example: Standard



11.3.2 Redirect Subscriber Login Screen

You can set the ZyXEL Device 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 **ADVANCED > CUSTOMIZATION > Login Page**, select **Redirect**.

Figure 39 ADVANCED > CUSTOMIZATION > Login Page: Redirect

The following table describes the related labels.

Table 17 ADVANCED > CUSTOMIZATION > 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 ZyXEL Device directs the subscribers for logins. The web site must be on the WAN. You can use up to 350 ASCII characters.
Code	Click **Code** to display the source code of the web page you specify. 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 ZyXEL Device.

Downloaded from www.Manualslib.com manuals search engine

Figure 40 ADVANCED > CUSTOMIZATION > Login Page: Redirect > Code

Redirect Login Page Code

```
<html>
<body style="font-family: Arial" bgcolor="#FFFFFF">
<form method="post" action="http://1.1.1.1/login.cgi" name="apply">
<div align="center">
<table cellSpacing="0" cellPadding="0" width="50%" borderColorLight="#8e8e8e"
border="1">
<tr>
<td align="center" width="100%" bgColor="#8e8e8e" height="24">
<font face="Arial, Helvetica, sans-serif" size="2" color="#FFFFFF"><b>Welcome</b></font>
</td>
</tr>
<tr>
<td align="center"> <table cellSpacing="0" cellPadding="4" width="100%"
bgColor="#FFFFFF" border="0"> <tr>
<td align="right" width="35%" style="font-family: Arial, Helvetica, sans-serif; font-size: 12pt">
<font color="#000000" size="2"><b>Username:</b></font>
</td>
<td width="65%">
<input type="text" name="username" size="25">
</td>
</tr>
<tr>
<td align="right" width="35%" style="font-family: Arial, Helvetica, sans-serif; font-size: 12pt">
<font color="#000000" size="2"><b>Password:</b></font>
</td>
<td width="65%">
<input type="password" name="password" size="25">
</td>
</tr>
<tr>
<td align="center" width="100%" style="font-family: Arial; font-size: 12pt" bgcolor="#F7F7F7"
colspan="2">
<input type="submit" name="apply" value="Enter" style="font-family: Arial">
<input type="reset" name="clear" value="Clear" style="font-family: Arial">
</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
</table>
</div>
</form>
</body>
</html>
```

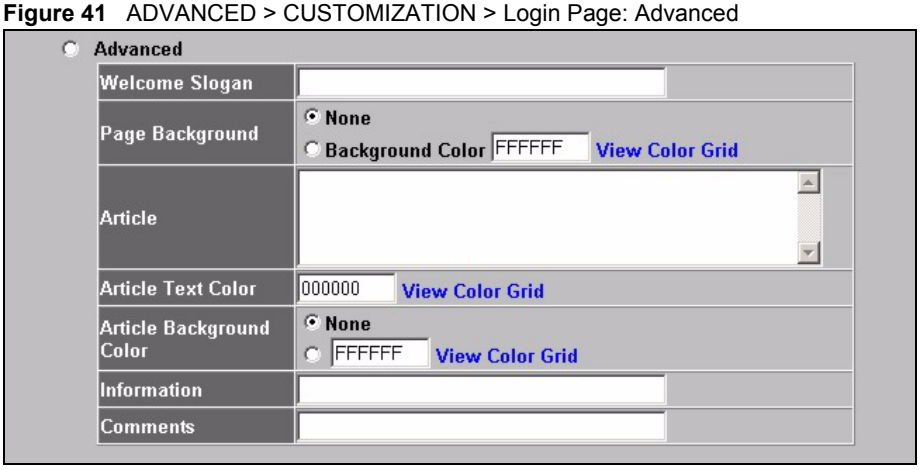
Close

11.3.3 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.

Downloaded from www.Manualslib.com manuals search engine

Figure 41 ADVANCED > CUSTOMIZATION > Login Page: Advanced



The following table describes the related labels.

Table 18 ADVANCED > CUSTOMIZATION > Login Page: Advanced

LABEL	DESCRIPTION
Advanced	Select this option to set the ZyXEL Device 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.
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.

Downloaded from www.Manualslib.com manuals search engine

Figure 42 ADVANCED > CUSTOMIZATION > Login Page: Advanced> View Color Grid

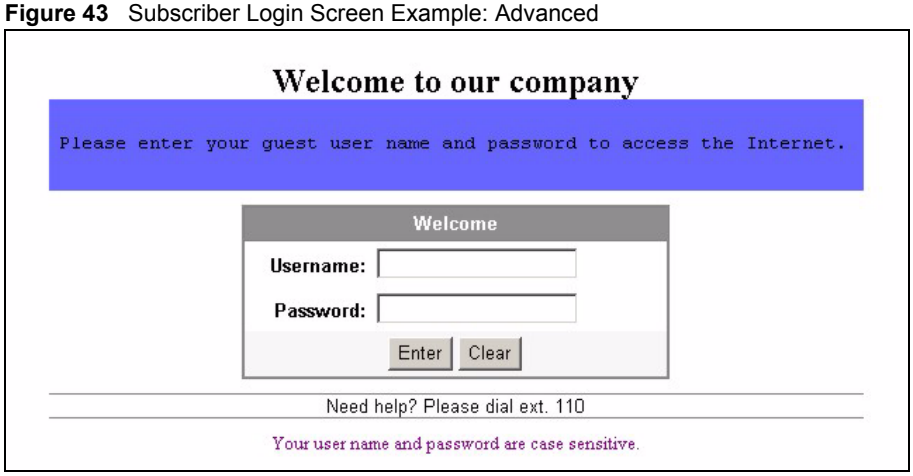
Browser Set Background Colors by RGB

		000066	000099	0000CC	0000FF
003300	003333	003366	003399	0033CC	0033FF
006600	006633	006666	006699	0066CC	0066FF
009900	009933	009966	009999	0099CC	0099FF
00CC00	00CC33	00CC66	00CC99	00CCCC	00CCFF
00FF00	00FF33	00FF66	00FF99	00FFCC	00FFFF
330000	330033	330066	330099	3300CC	3300FF
333300	333333	333366	333399	3333CC	3333FF
336600	336633	336666	336699	3366CC	3366FF
339900	339933	339966	339999	3399CC	3399FF
33CC00	33CC33	33CC66	33CC99	33CCCC	33CCFF
33FF00	33FF33	33FF66	33FF99	33FFCC	33FFFF
660000	660033	660066	660099	6600CC	6600FF
663300	663333	663366	663399	6633CC	6633FF
666600	666633	666666	666699	6666CC	6666FF
669900	669933	669966	669999	6699CC	6699FF
66CC00	66CC33	66CC66	66CC99	66CCCC	66CCFF
66FF00	66FF33	66FF66	66FF99	66FFCC	66FFFF
990000	990033	990066	990099	9900CC	9900FF
993300	993333	993366	993399	9933CC	9933FF
996600	996633	996666	996699	9966CC	9966FF
999900	999933	999966	999999	9999CC	9999FF
99CC00	99CC33	99CC66	99CC99	99CCCC	99CCFF
99FF00	99FF33	99FF66	99FF99	99FFCC	99FFFF
CC0000	CC0033	CC0066	CC0099	CC00CC	CC00FF
CC3300	CC3333	CC3366	CC3399	CC33CC	CC33FF
CC6600	CC6633	CC6666	CC6699	CC66CC	CC66FF
CC9900	CC9933	CC9966	CC9999	CC99CC	CC99FF
CCCC00	CCCC33	CCCC66	CCCC99	CCCCCC	CCCCFF
CCFF00	CCFF33	CCFF66	CCFF99	CCFFCC	CCFFFF
FF0000	FF0033	FF0066	FF0099	FF00CC	FF00FF
FF3300	FF3333	FF3366	FF3399	FF33CC	FF33FF
FF6600	FF6633	FF6666	FF6699	FF66CC	FF66FF
FF9900	FF9933	FF9966	FF9999	FF99CC	FF99FF
FFCC00	FFCC33	FFCC66	FFCC99	FFCCCC	FFCCFF
FFFF00	FFFF33	FFFF66	FFFF99	FFFFCC	FFFFFF

The following figure shows an advanced subscriber login screen example.

Downloaded from www.Manualslib.com manuals search engine

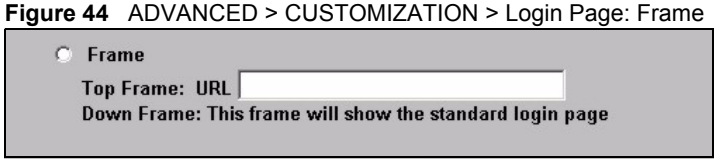
Figure 43 Subscriber Login Screen Example: Advanced



11.3.4 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 44 ADVANCED > CUSTOMIZATION > Login Page: Frame



The following table describes the related labels.

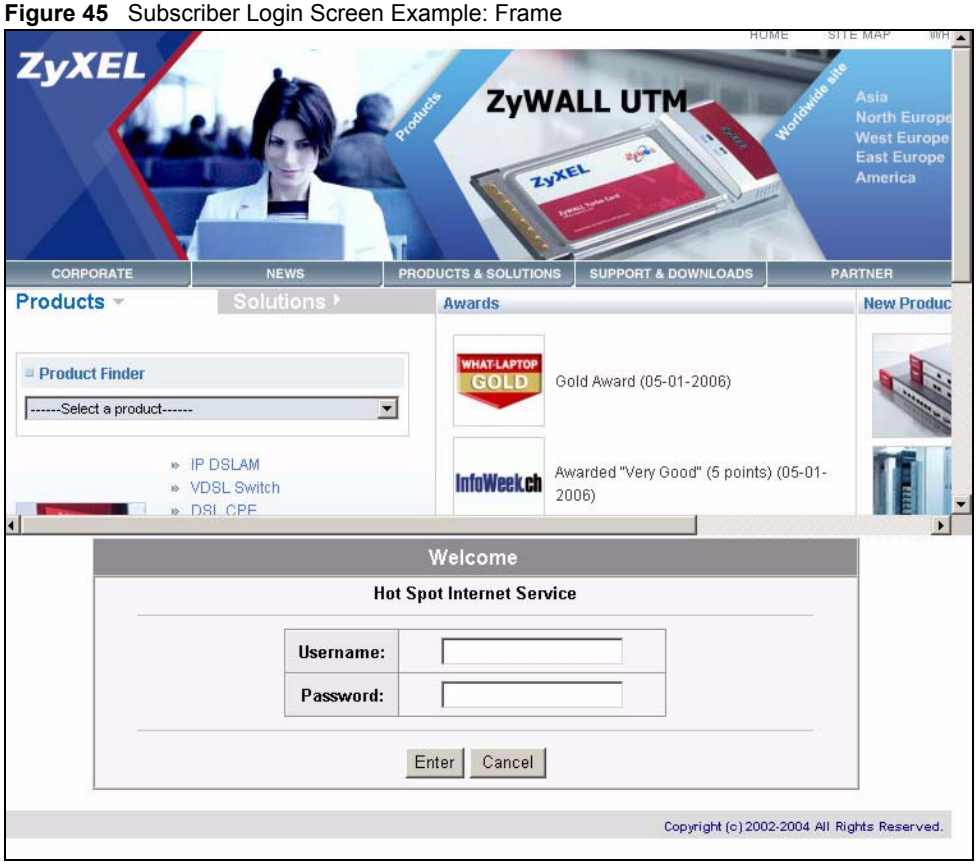
Table 19 ADVANCED > CUSTOMIZATION > Login Page: Frame

label	description
Frame	Select this option to configure and set the ZyXEL Device 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. You can use up to 350 ASCII characters.
Down Frame	The bottom frame displays the standard subscriber login page.

The following figure shows a framed subscriber login screen example.

Downloaded from www.Manualslib.com manuals search engine

Figure 45 Subscriber Login Screen Example: Frame



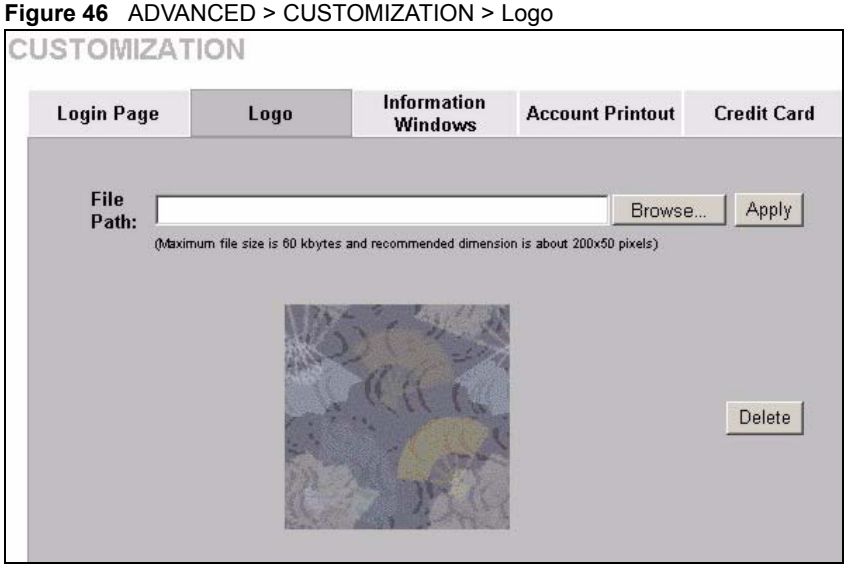
11.4 Adding a Logo

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 > Logo** to display the screen as shown next.

Downloaded from www.Manualslib.com manuals search engine

Figure 46 ADVANCED > CUSTOMIZATION > Logo



The following table describes the labels in this screen.

Table 20 ADVANCED > CUSTOMIZATION > Logo

LABEL	DESCRIPTION
File Path	Enter the file path name of the logo file or click **Browse** to search for it.
Apply	Click **Apply** to upload your logo file to the ZyXEL Device.
Delete	Click **Delete** to remove the logo you uploaded.

11.5 About the Information Windows

You can set the ZyXEL Device 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 ZyXEL Device.

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.

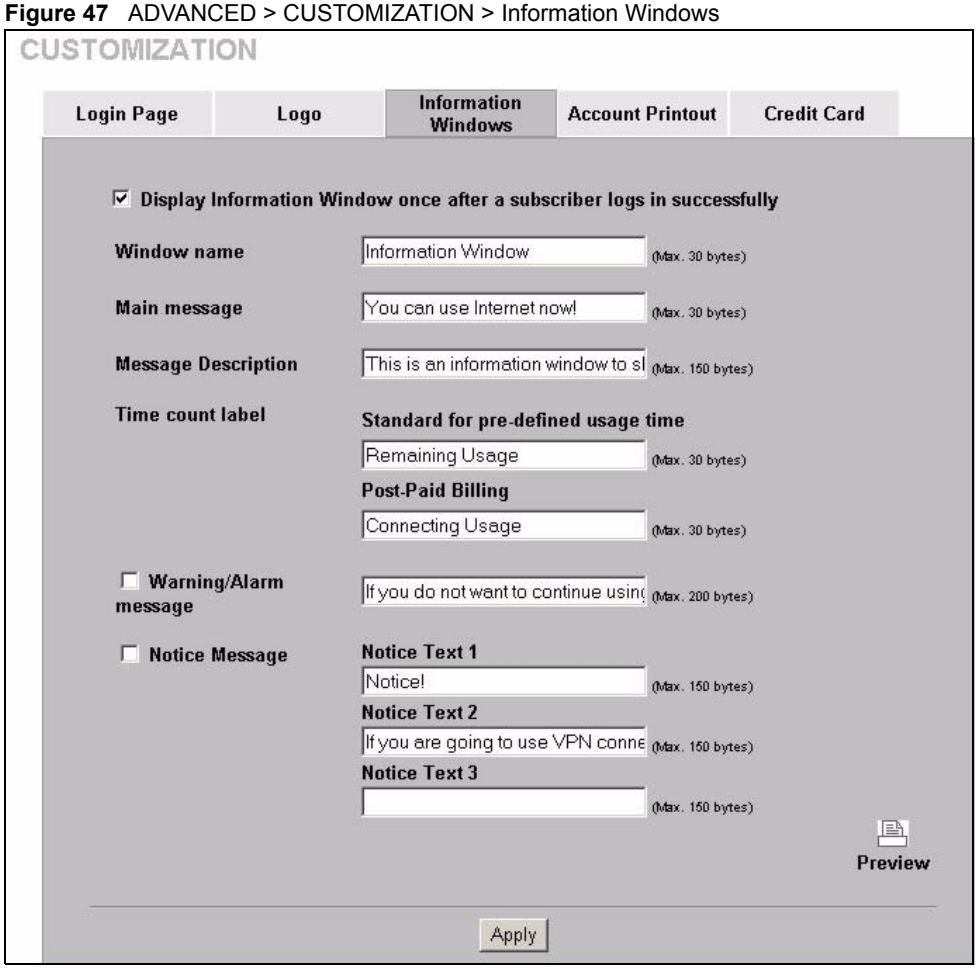
Downloaded from www.Manualslib.com manuals search engine

11.5.1 Customizing the Information Windows

Click **ADVANCED > CUSTOMIZATION > Information Windows** to display the screen as shown next.

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

Figure 47 ADVANCED > CUSTOMIZATION > Information Windows



The following table describes the labels in this screen.

Table 21 ADVANCED > CUSTOMIZATION > Information Windows

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).

Downloaded from www.Manualslib.com manuals search engine

Table 21 ADVANCED > CUSTOMIZATION > Information Windows (continued)

LABEL	DESCRIPTION
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 ZyXEL Device 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 ZyXEL Device 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.

11.6 About the Account Printout

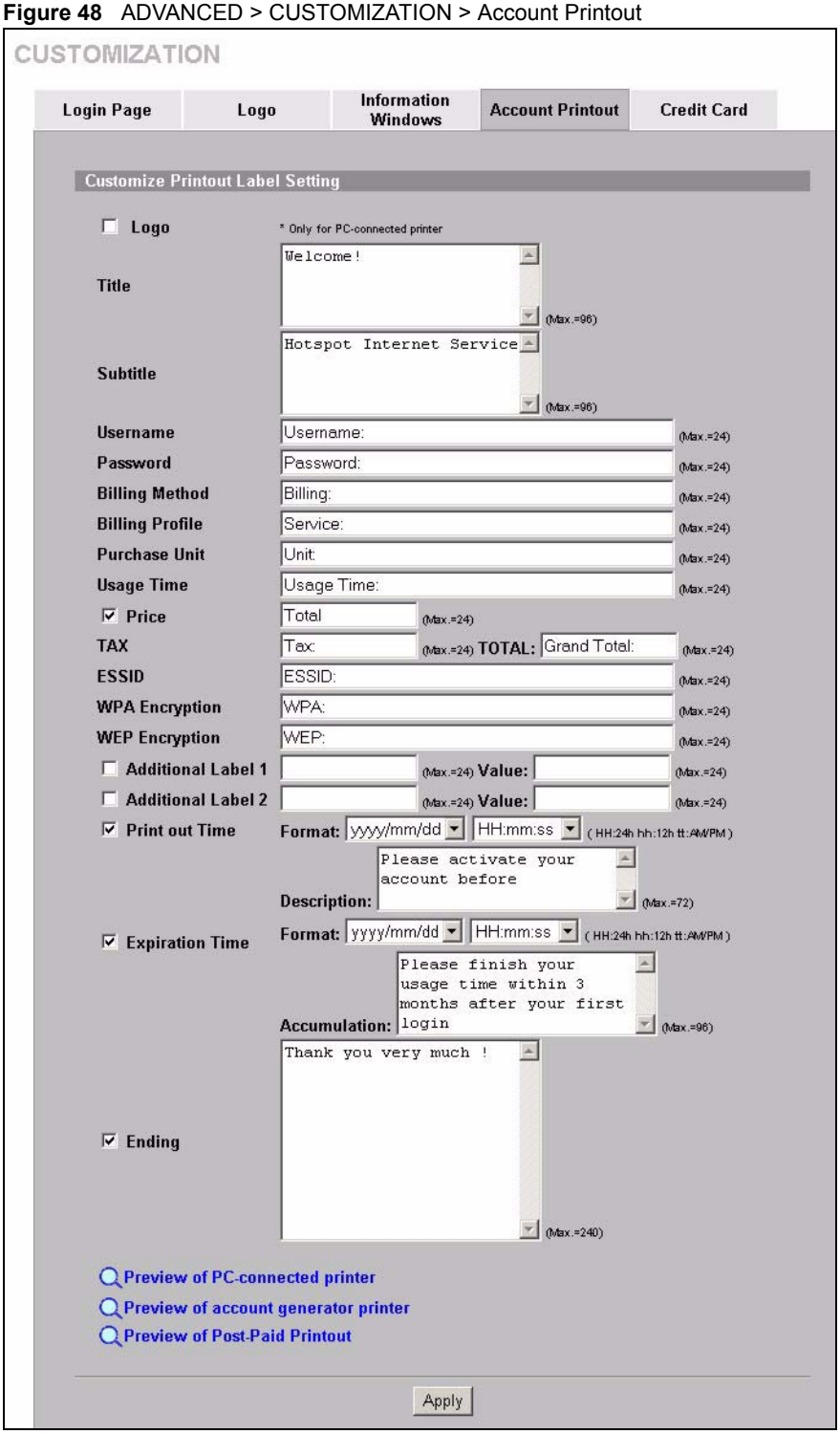
After you have created the subscriber accounts, you can print out the account information.

11.6.1 Customizing the Account Printout

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

Downloaded from www.Manualslib.com manuals search engine

Figure 48 ADVANCED > CUSTOMIZATION > Account Printout



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 22 ADVANCED > CUSTOMIZATION > 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 11.4 on page 109 for how to upload a logo file.
Title	Enter a title for the printout.
Subtitle	Enter a subtitle for the printout.
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**).
WPA Encryption	Type a label name for the field displaying the Wi-Fi Protected Access (**WPA Encryption**) key. This field displays on the account statement when the ZyXEL Device is using WPA data encryption with a pre-shared key.
WEP Encryption	Type a label name for the field displaying the Wired Equivalent Privacy (**WEP Encryption**) key. This field displays on the account statement when the ZyXEL Device is using WEP data encryption.
Additional Label 1 and 2	Select this check box to display the specified label name(s) for the field(s) displaying any additional information.
Value	Type any additional information that you want to display.
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.
Accumulation	This message displays in the account printout when you set the ZyXEL Device to use accumulation billing. Enter an explanation for the subscriber about the deadline for using the purchased time.
Ending	Select this check box to display a message at the end of the printout. Enter the message 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.

Downloaded from www.Manualslib.com manuals search engine

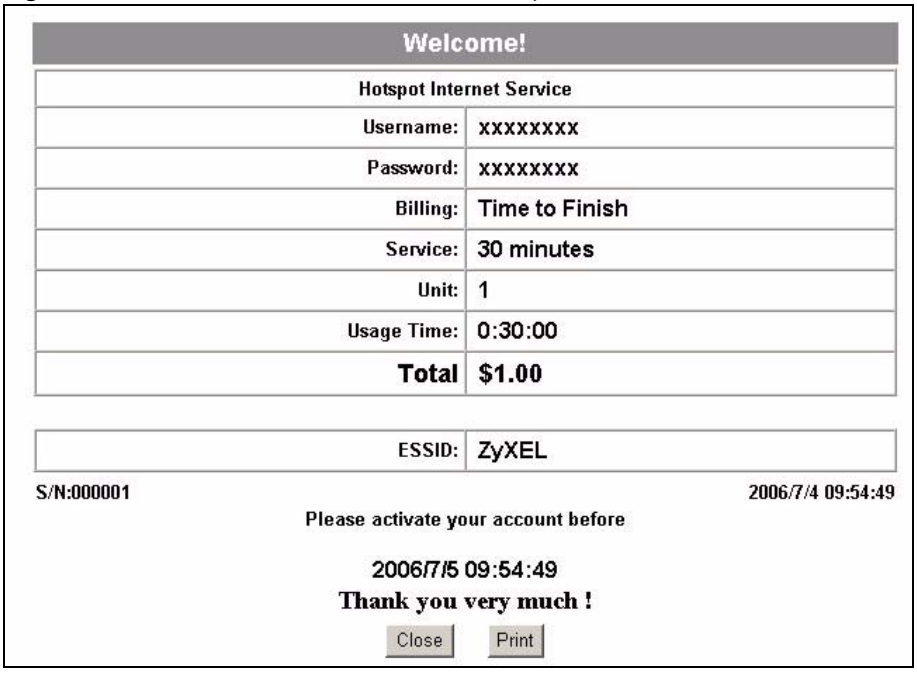
Table 22 ADVANCED > CUSTOMIZATION > Account Printout (continued)

LABEL	DESCRIPTION
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).
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.

Downloaded from www.Manualslib.com manuals search engine

Figure 49 Preview of PC-connected Printer Example



Welcome!

Hotspot Internet Service	
Username:	xxxxxxxx
Password:	xxxxxxxx
Billing:	Time to Finish
Service:	30 minutes
Unit:	1
Usage Time:	0:30:00
Total	**$1.00**

ESSID:	ZyXEL

S/N:000001 2006/7/4 09:54:49

Please activate your account before

2006/7/5 09:54:49

Thank you very much !

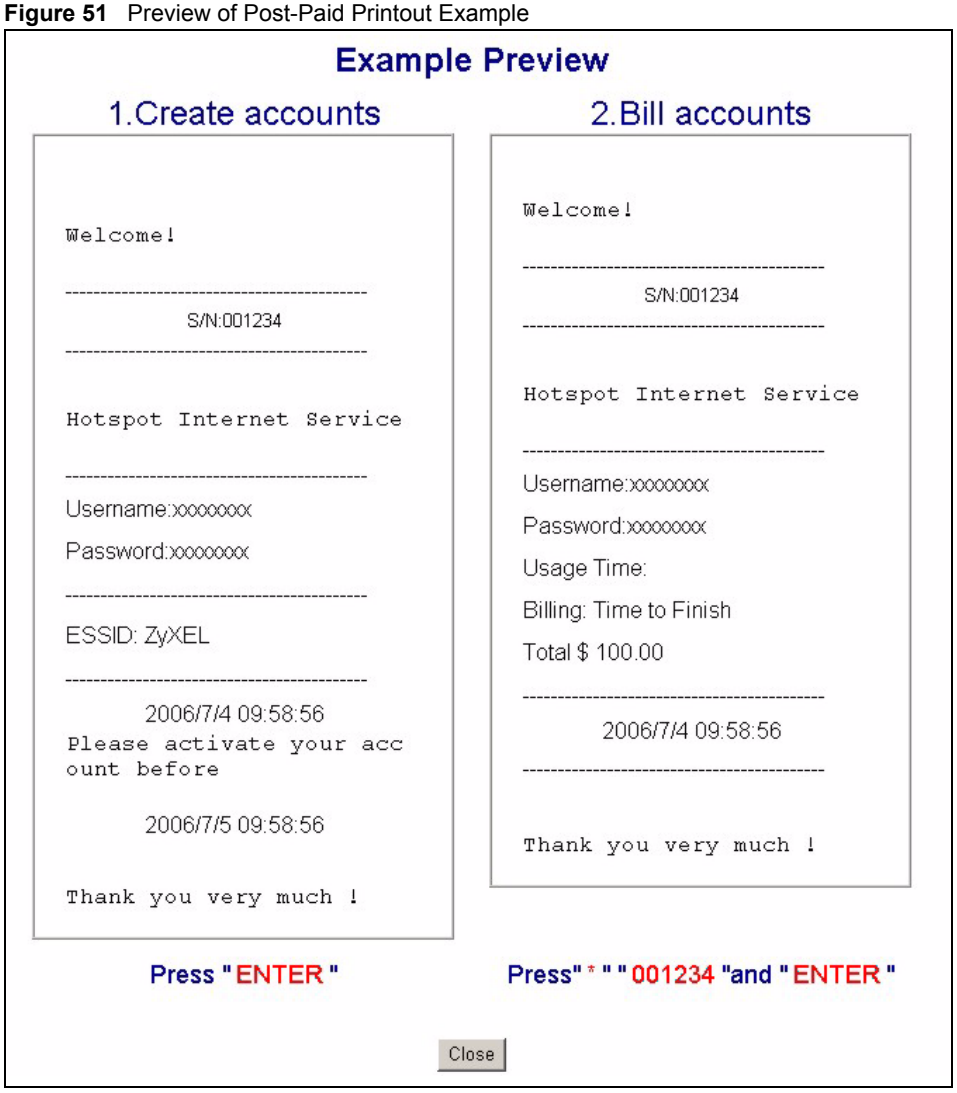
Close Print

Downloaded from www.Manualslib.com manuals search engine

Figure 50 Preview of Account Generator Printer Example

Downloaded from www.Manualslib.com manuals search engine

Figure 51 Preview of Post-Paid Printout Example



11.7 Customizing the Credit Card

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

11.7.1 Credit Card Standard Login Page

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

Downloaded from www.Manualslib.com manuals search engine

Figure 52 ADVANCED > CUSTOMIZATION > Credit Card: Standard Login Page

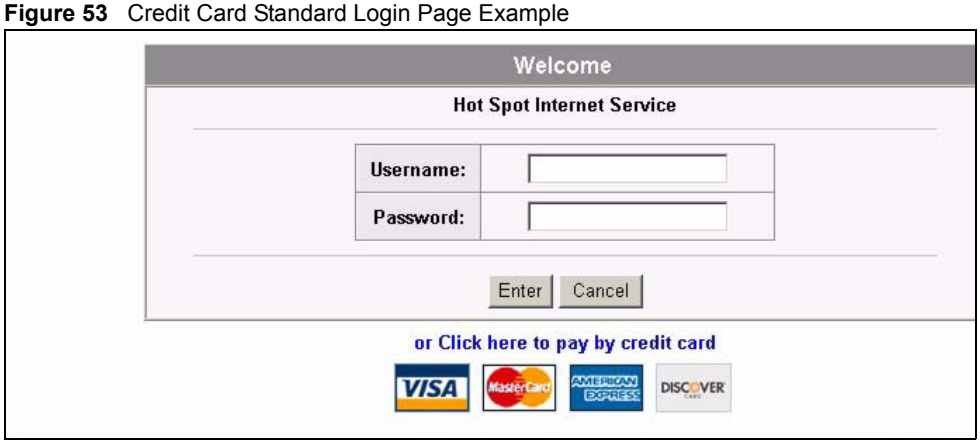
The following table describes the labels in this section.

Table 23 ADVANCED > CUSTOMIZATION > Credit Card: Standard Login Page

LABEL	DESCRIPTION
Credit Card Message	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 53 Credit Card Standard Login Page Example

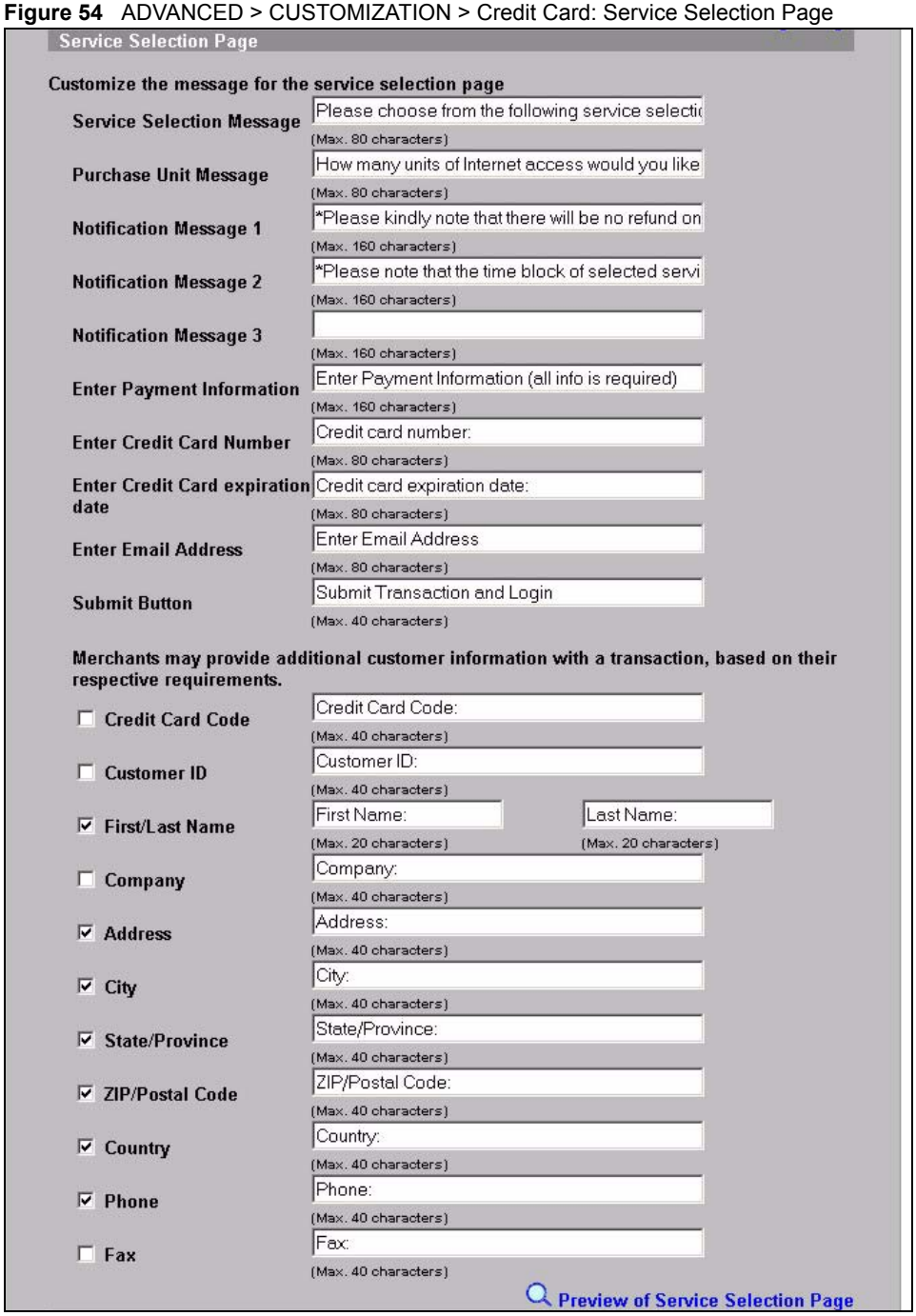


11.7.2 Credit Card Service Selection Page

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

Downloaded from www.Manualslib.com manuals search engine

Figure 54 ADVANCED > CUSTOMIZATION > Credit Card: Service Selection Page



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this section.

Table 24 ADVANCED > CUSTOMIZATION > 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.
Credit Card Code	Credit cards have an authorization code on the back. Select this check box if you want the screen to display a credit card authorization code field. Enter the label name for the field that requests the subscriber's credit card authorization code.
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.
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.

Downloaded from www.Manualslib.com manuals search engine

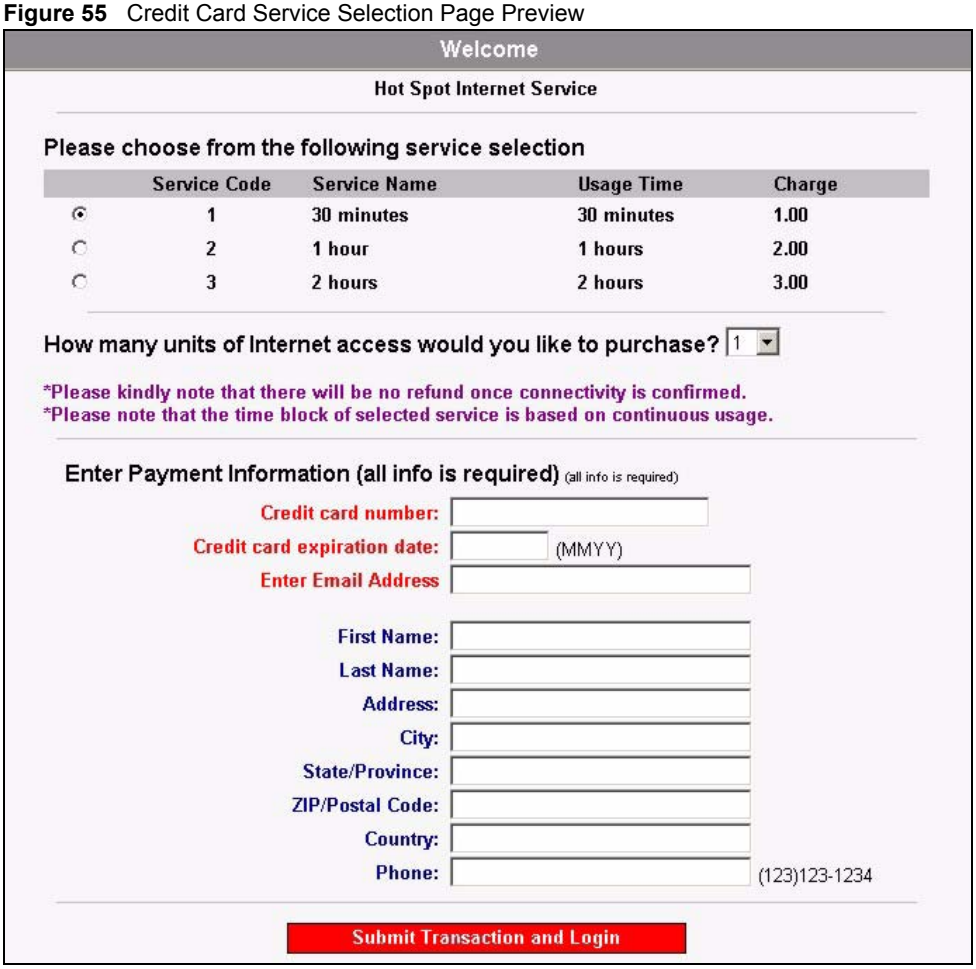
Table 24 ADVANCED > CUSTOMIZATION > Credit Card: Service Selection Page

LABEL	DESCRIPTION
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.

Downloaded from www.Manualslib.com manuals search engine

Figure 55 Credit Card Service Selection Page Preview

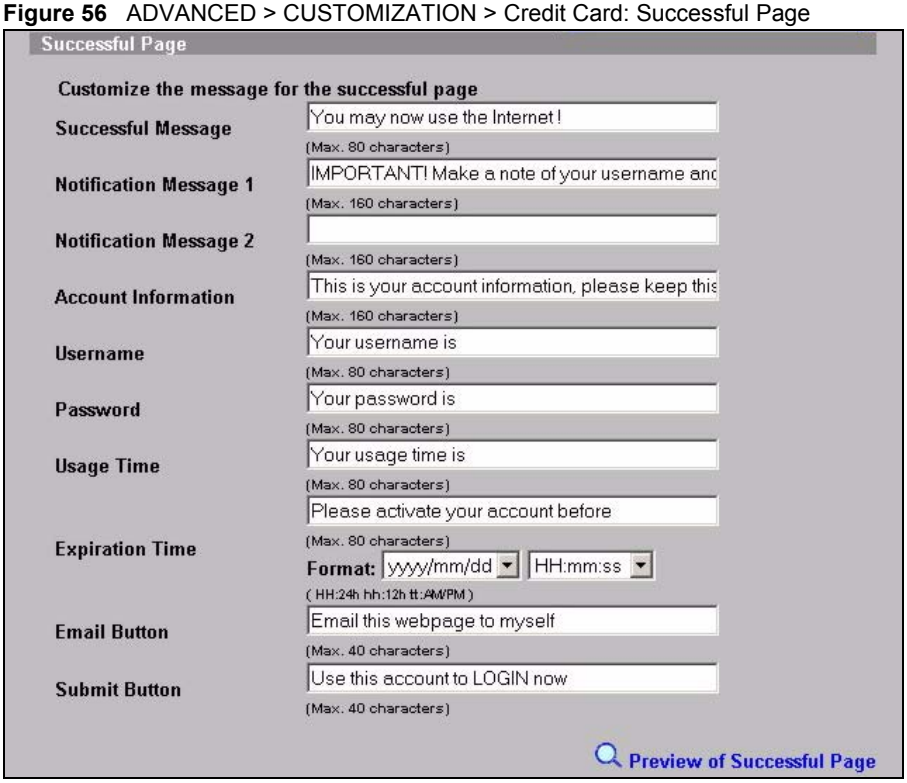


11.7.3 Credit Card Successful Page

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

Downloaded from www.Manualslib.com manuals search engine

Figure 56 ADVANCED > CUSTOMIZATION > Credit Card: Successful Page



The following table describes the labels in this section.

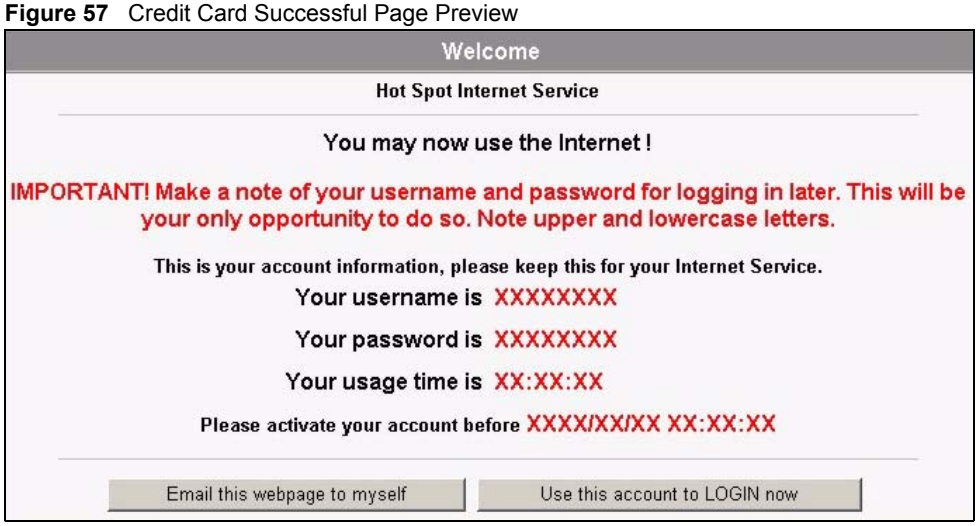
Table 25 ADVANCED > CUSTOMIZATION > Credit Card: Successful Page

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.
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.

Downloaded from www.Manualslib.com manuals search engine

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

Figure 57 Credit Card Successful Page Preview

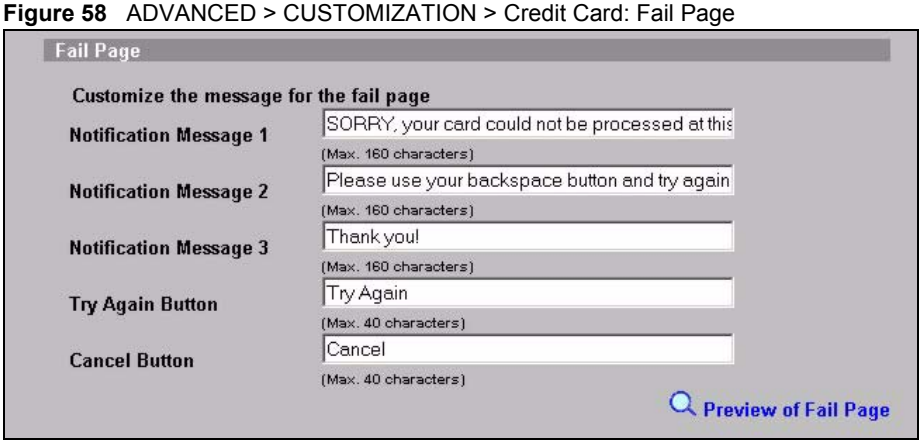


11.7.4 Credit Card Fail Page

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

Downloaded from www.Manualslib.com manuals search engine

Figure 58 ADVANCED > CUSTOMIZATION > Credit Card: Fail Page



The following table describes the labels in this section.

Table 26 ADVANCED > CUSTOMIZATION > Credit Card: 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.
Cancel 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 59 Credit Card Failed Page Preview

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 12
Pass Through

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

12.1 About the Pass Through

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

You can set the ZyXEL Device 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.

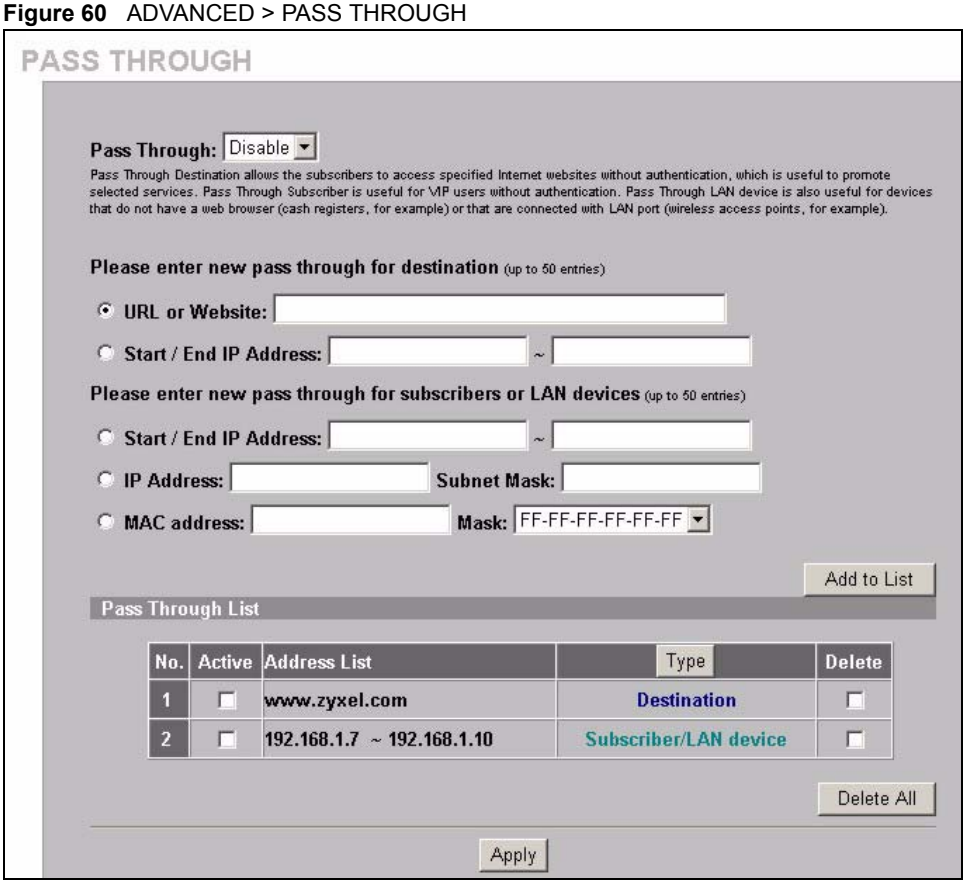
12.2 Configuring Pass Through

To configure pass through on the ZyXEL Device, click **ADVANCED > PASS THROUGH**.

Note: Pass through has priority over filtering.

Downloaded from www.Manualslib.com manuals search engine

Figure 60 ADVANCED > PASS THROUGH



The following table describes the labels in this screen.

Table 27 ADVANCED > 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 ZyXEL Device 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.
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 350 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)

Downloaded from www.Manualslib.com manuals search engine

Table 27 ADVANCED > PASS THROUGH (continued)

LABEL	DESCRIPTION
Start / End IP Address	Select this option to allow packets from computers with a specific range of IP addresses to pass through the ZyXEL Device 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 ZyXEL Device 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 ZyXEL Device 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 ZyXEL Device.
No.	This read-only field displays the index number of a pass through entry.
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.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 13
Filtering

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

13.1 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.

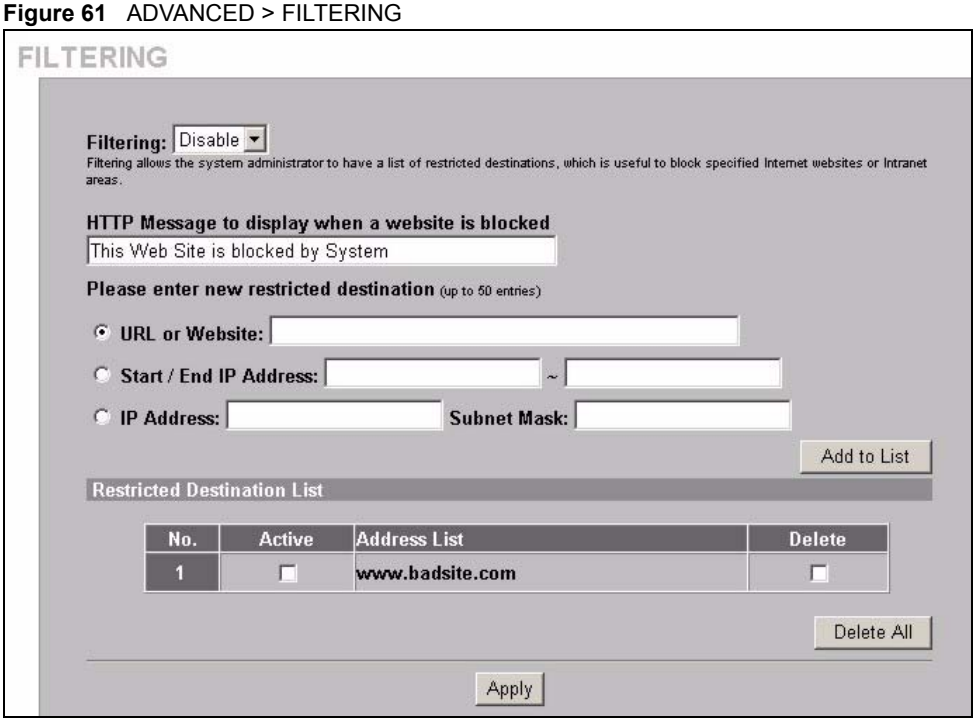
13.2 Configuring Filtering

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

Note: Pass through has priority over filtering.

Downloaded from www.Manualslib.com manuals search engine

Figure 61 ADVANCED > FILTERING



The following table describes the related labels.

Table 28 ADVANCED > 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".
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 350 ASCII 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.

Downloaded from www.Manualslib.com manuals search engine

Table 28 ADVANCED > FILTERING (continued)

LABEL	DESCRIPTION
Active	Select this check box to block subscriber access to this destination.
Address List	This field displays the destination address(s).
Delete	Select this(ese) 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.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 14
Share

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

14.1 About Share

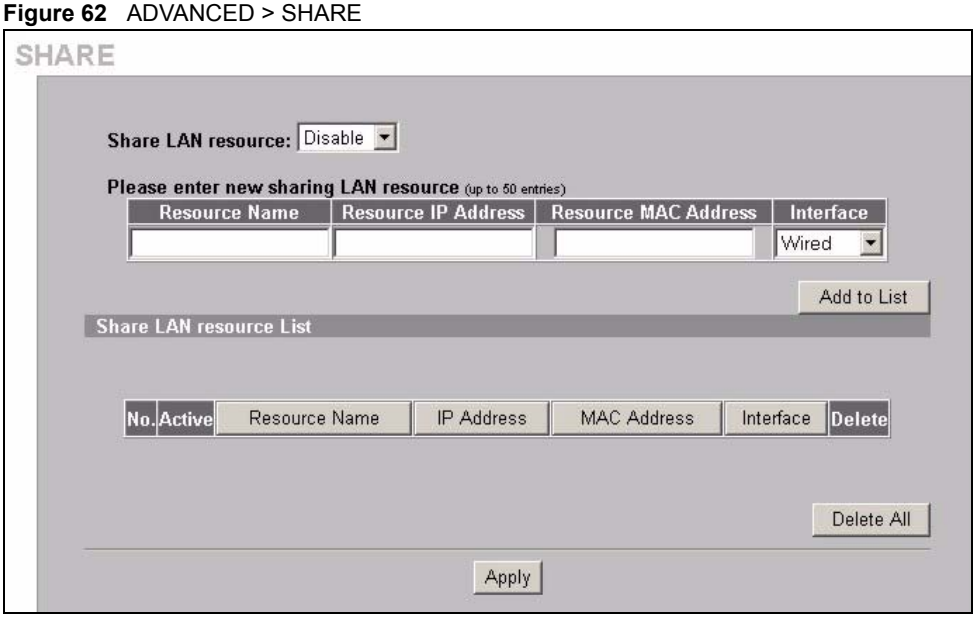
The share function allows logged-in subscribers to share devices on the LAN. This is useful for allowing subscribers to use printers or servers.

14.2 Configuring Share

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

Downloaded from www.Manualslib.com manuals search engine

Figure 62 ADVANCED > SHARE



The following table describes the related labels.

Table 29 ADVANCED > 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.
Resource MAC Address	Enter the MAC address of the LAN device.
Interface	Select the ZyXEL Device'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.

Downloaded from www.Manualslib.com manuals search engine

Table 29 ADVANCED > SHARE (continued)

LABEL	DESCRIPTION
Interface	This field displays to which of the ZyXEL Device'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(ies).
Delete All	Click this button to remove all of the share device entries.
Apply	Click **Apply** to save the changes.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 15
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.

15.1 Portal Page Advertisement Links and Walled Garden Overview

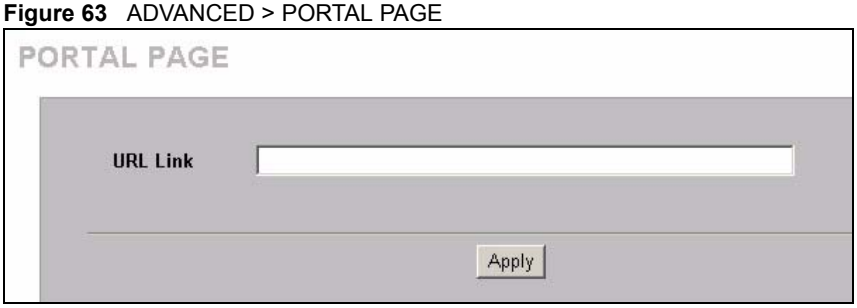
When you enable subscriber authentication in the **Authentication Configuration** screen, you can set the ZyXEL Device to redirect a subscriber to a portal web site, display advertisement links or activate the walled garden feature for generating on-line advertising revenue.

15.2 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 ZyXEL Device 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 > PORTAL PAGE** to display the screen as shown next.

Figure 63 ADVANCED > PORTAL PAGE



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

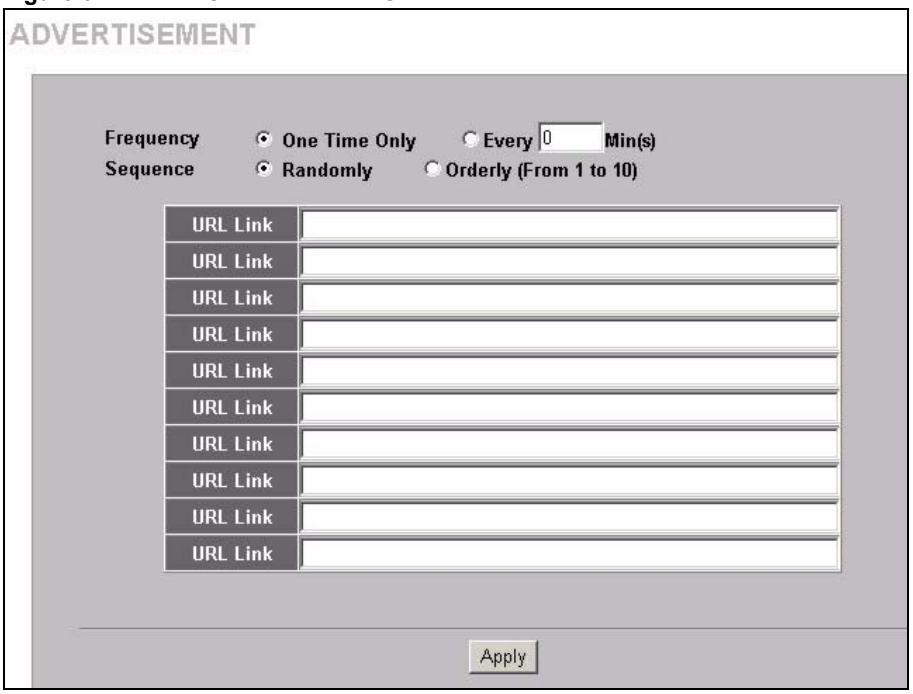
Table 30 ADVANCED > PORTAL PAGE

LABEL	DESCRIPTION
URL Link	Enter the web site address of a portal page. You can use up to 350 ASCII characters.
Apply	Click **Apply** to save the settings.

15.3 Advertisement Links

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

Figure 64 ADVANCED > ADVERTISEMENT



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 31 ADVANCED > ADVERTISEMENT

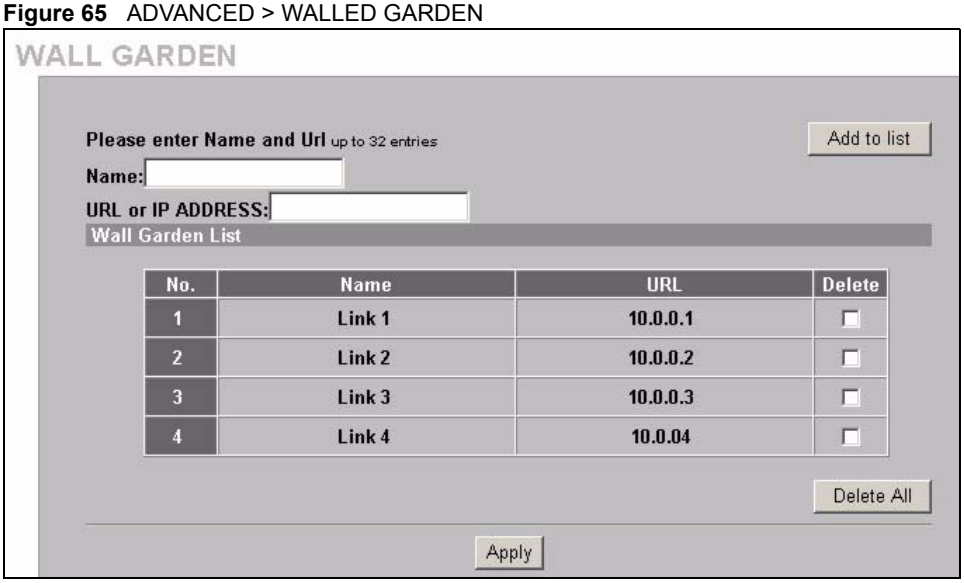
LABEL	DESCRIPTION
Frequency	Select **One Time Only** to display an advertisement web site in an active browser window once after a subscriber logs in successfully. Select **Every … Min(s)** to display an advertisement web site in an active browser window once every time period specified (in minutes) after a subscriber logs in successfully.
Sequence	Select **Randomly** to display the advertisement links in random order, one at a time. Select **Orderly** to display the advertisement links in the order that you configure them.
URL Link	Enter the web site URLs in the fields provided. For example, "http://www.zyxel.com". You can use up to 350 ASCII characters.
Apply	Click **Apply** to save the changes.

15.4 Walled Garden

A subscriber must log in before the ZyXEL Device allows the subscriber access to the Internet. However, with a walled garden, you can define one or more web site addresses that all subscribers can access without logging in. These can be used for advertisements for example.

Click **ADVANCED > WALLED GARDEN** to display the screen as shown.

Figure 65 ADVANCED > WALLED GARDEN



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

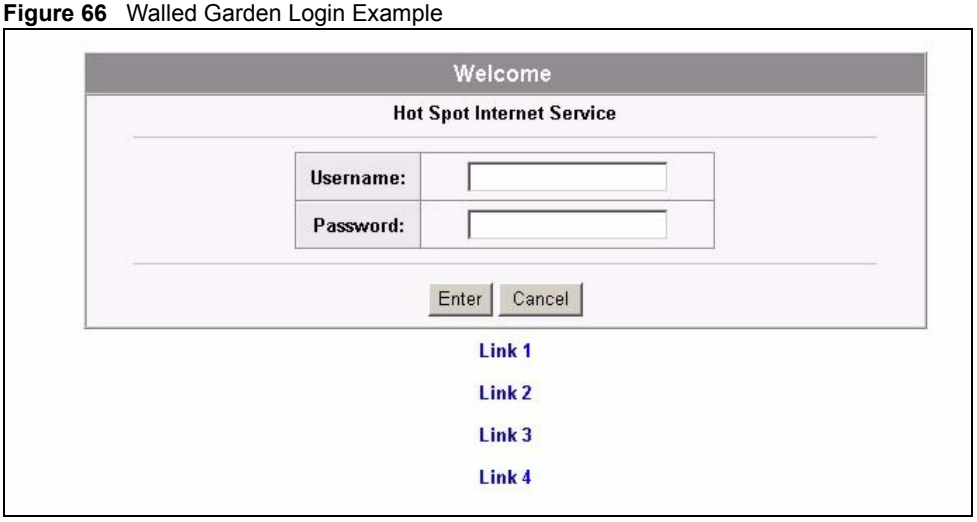
Table 32 ADVANCED > WALLED GARDEN

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 80 characters) for the walled garden link to be displayed in the web browser.
URL or IP Address	Enter the web site URL (up to 350 ASCII characters) or IP address. For example, "http://www.zyxel.com".
Add to List	Click this button to append your entry to the list below.
Delete	Select the check boxes of entries that you want to remove and click **Apply** to remove them.
Delete All	Click this button to remove all of the walled garden links.
Apply	Click **Apply** to save the changes.

15.4.1 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.

Figure 66 Walled Garden Login Example



Downloaded from www.Manualslib.com manuals search engine

CHAPTER 16
DDNS

This chapter shows you how to set the ZyXEL Device to use DDNS.

16.1 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 ZyXEL Device 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.

Note: 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 ZyXEL Device.

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

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

16.1.1 DYNDNS Wildcard

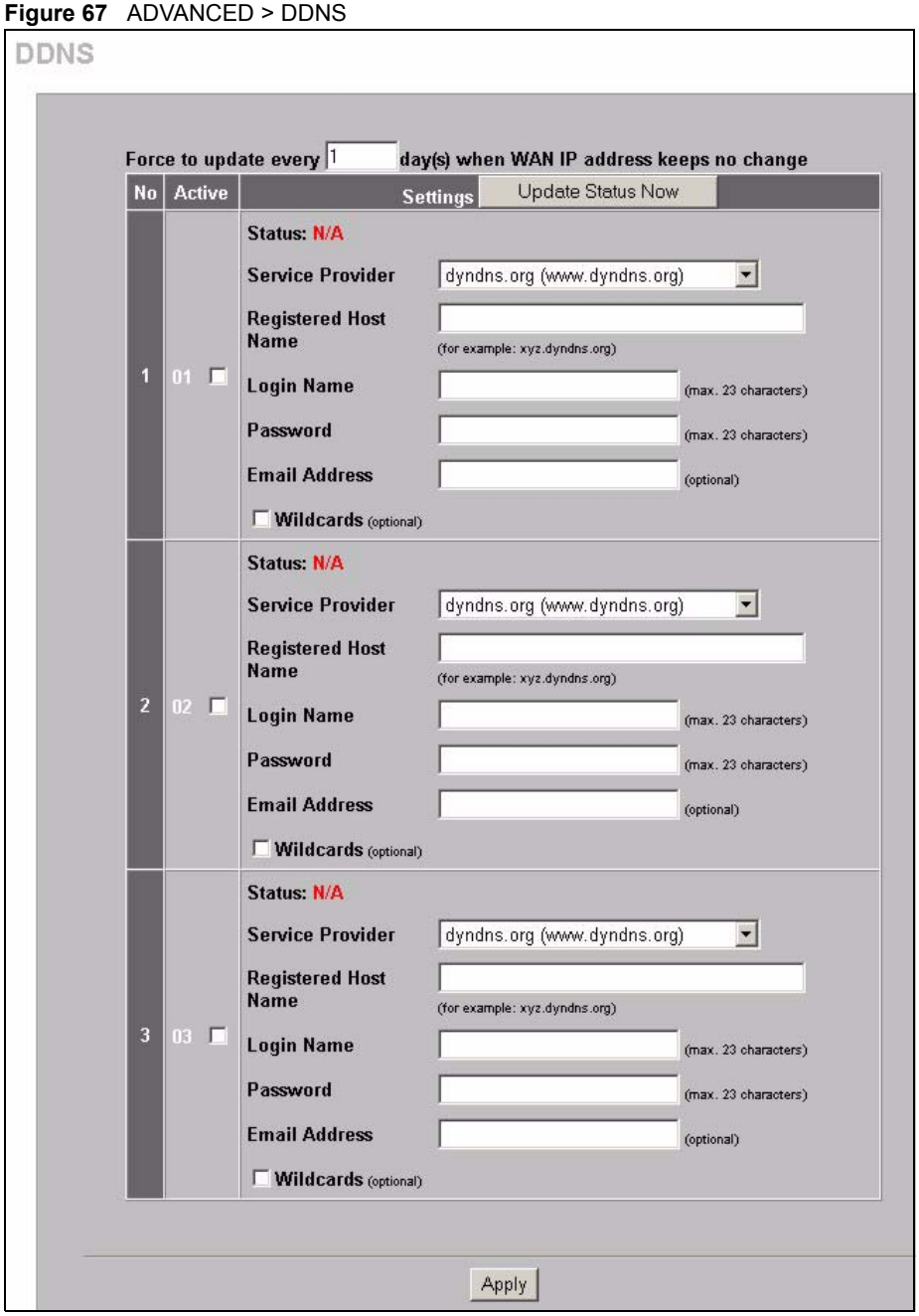
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

16.2 Configuring DDNS

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

Downloaded from www.Manualslib.com manuals search engine

Figure 67 ADVANCED > DDNS



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 33 ADVANCED > 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 ZyXEL Device updates the DDNS server with the ZyXEL Device's WAN IP address when the ZyXEL Device'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 ZyXEL Device update the DDNS server with the ZyXEL Device'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.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 17
LAN Devices

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

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

17.1.1 Port Mapping

To make LAN devices behind the ZyXEL Device visible to the outside world, you configure a mapping between a virtual port on the ZyXEL Device and a server port on a LAN device. A virtual port is a port on the ZyXEL Device 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 ZyXEL Device using port mapping. You can access the management interface on the LAN device remotely provided that the LAN device has allowed remote management.

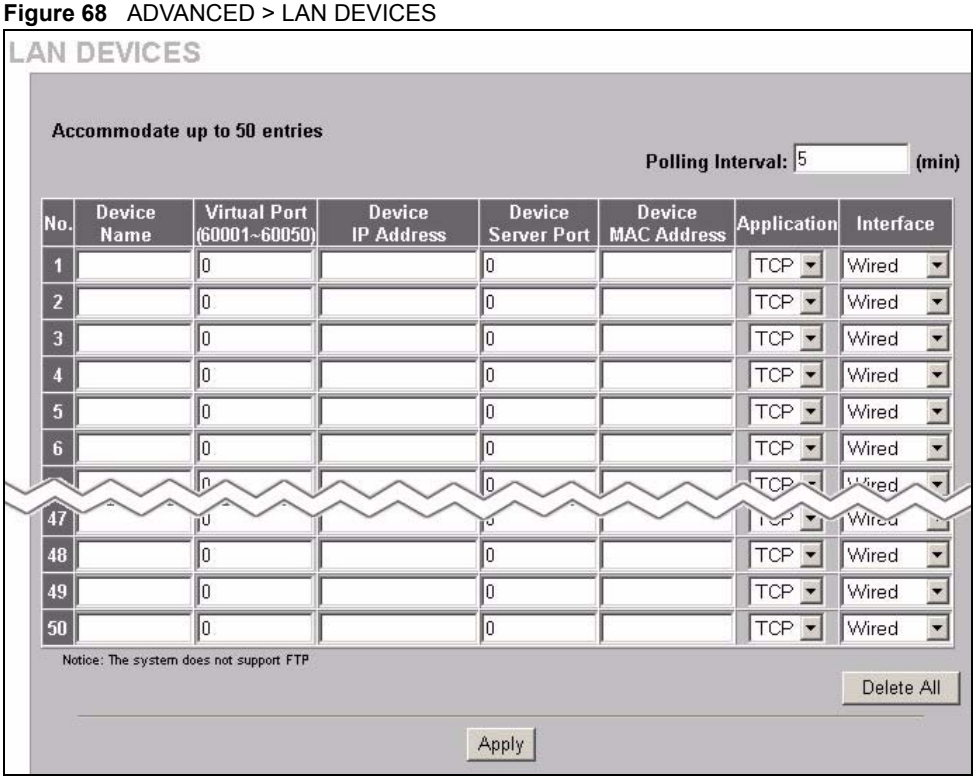
17.2 Configuring LAN Devices Port Mapping

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

Note: You can configure port mapping for up to 50 LAN devices on the ZyXEL Device.

Downloaded from www.Manualslib.com manuals search engine

Figure 68 ADVANCED > LAN DEVICES



The following table describes the labels in this screen.

Table 34 ADVANCED > LAN DEVICES

LABEL	DESCRIPTION
Polling Interval	Specify the time interval (in minutes) between the ZyXEL Device'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.
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 ZyXEL Device's interface to which the LAN device is connected.

Downloaded from www.Manualslib.com manuals search engine

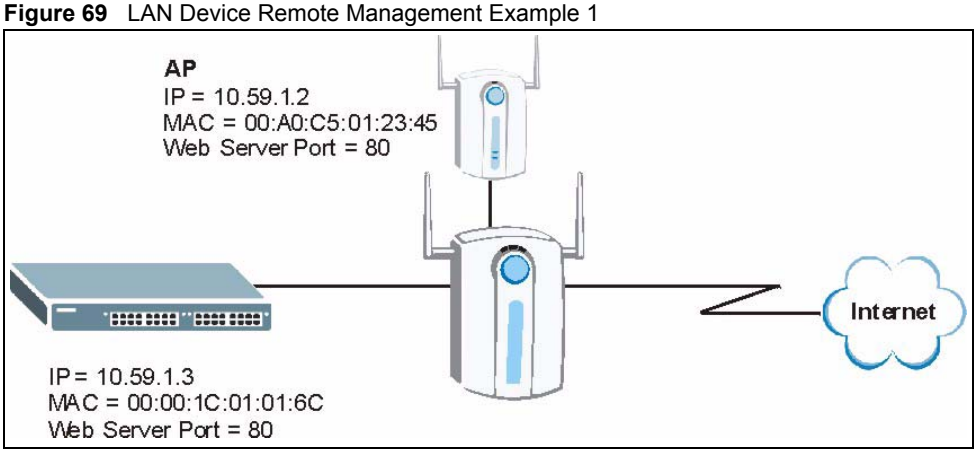
Table 34 ADVANCED > LAN DEVICES (continued)

LABEL	DESCRIPTION
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.

17.2.1 LAN Device Management Example

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

Figure 69 LAN Device Remote Management Example 1



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

Figure 70 ADVANCED > LAN DEVICES: Example 1

LAN DEVICES

Accommodate up to 50 entries

Polling Interval: 5 (min)

No.	Device Name	Virtual Port (60001~60050)	Device IP Address	Device Server Port	Device MAC Address	Application	Interface
1	AP	60001	10.59.1.2	80	00ADC5012345	TCP	Wired
2	Switch	60002	10.59.1.3	80	00001C01016C	TCP	Wired
3		0		0		TCP	Wired

Downloaded from www.Manualslib.com manuals search engine

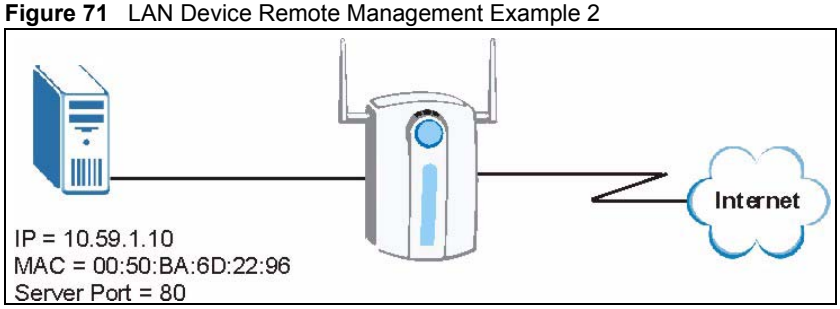
To access the web-based management interface, enter the WAN IP address of your ZyXEL Device and the virtual port number of the LAN device separated by a colon. In this example, to access the access point (AP), enter "http:// 192.168.1.1:60001" where 192.168.1.1 is the WAN IP address of the ZyXEL Device.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

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

17.2.2 Specifying an Inside Server Example

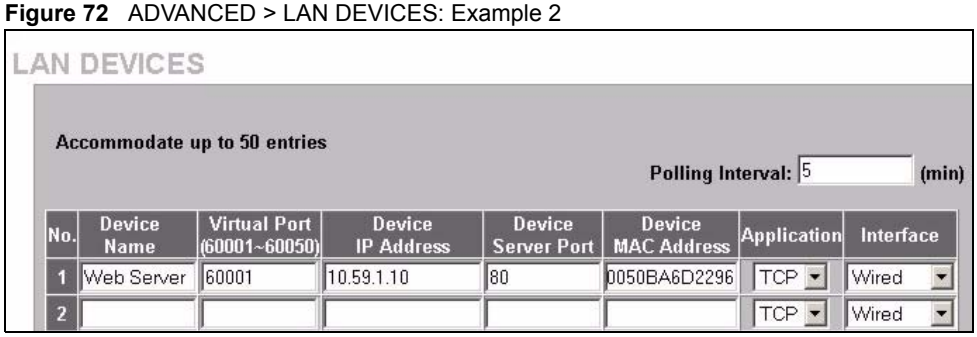
Let's say you have a web server behind the ZyXEL Device as shown in the next figure.

Figure 71 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 72 ADVANCED > LAN DEVICES: Example 2



No.	Device Name	Virtual Port (60001~60050)	Device IP Address	Device Server Port	Device MAC Address	Application	Interface
1	Web Server	60001	10.59.1.10	80	0050BA6D2296	TCP	Wired
2						TCP	Wired

To access an inside server on the LAN, enter the WAN IP address of your ZyXEL Device 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 ZyXEL Device.

You can also access the server by entering the domain name provided that the ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

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

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 18
Syslog

This chapter shows you how to configure syslog on the ZyXEL Device.

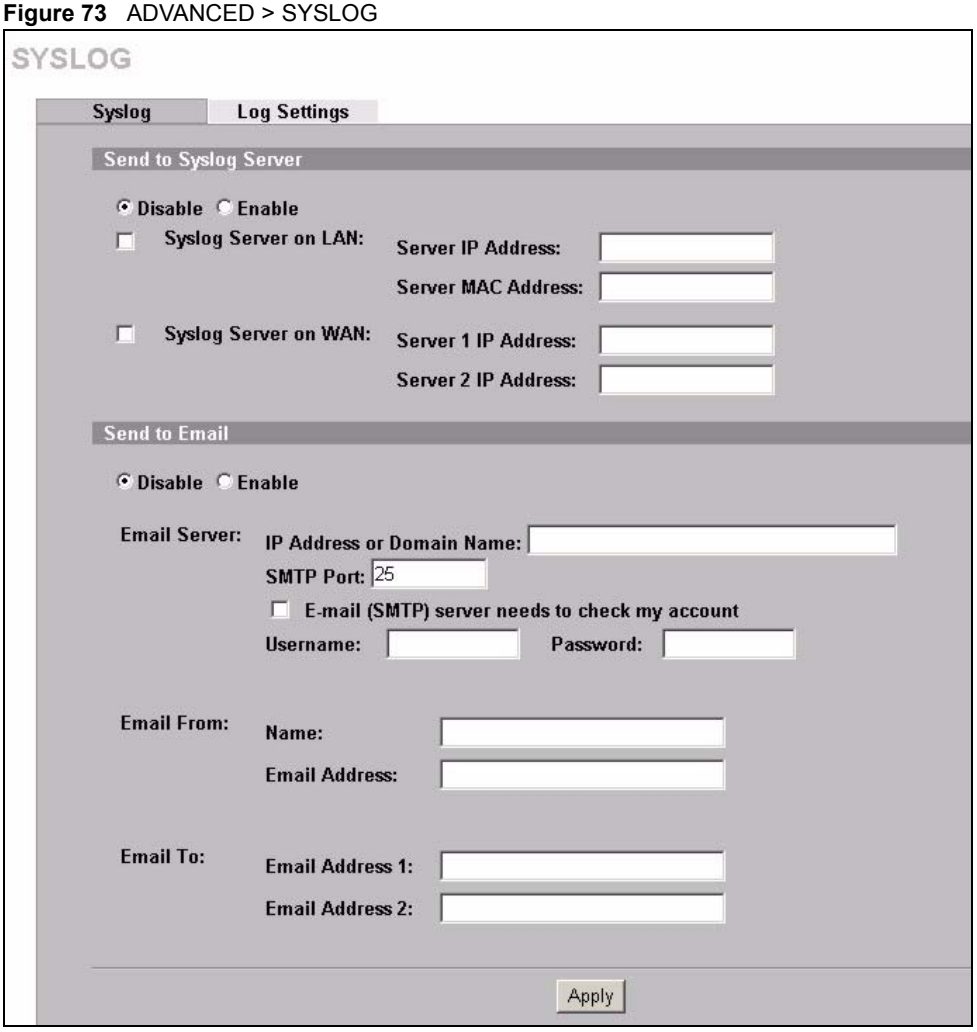
18.1 Syslog Configuration

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

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

Downloaded from www.Manualslib.com manuals search engine

Figure 73 ADVANCED > SYSLOG



The following table describes the labels in this screen.

Table 35 ADVANCED > 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.

Downloaded from www.Manualslib.com manuals search engine

Table 35 ADVANCED > SYSLOG (continued)

LABEL	DESCRIPTION
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 ZyXEL Device send syslog messages to the e-mail account that you specify. Select **Disable** to not have the ZyXEL Device 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 ZyXEL Device sends.
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 ZyXEL Device 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.

18.2 Syslog Log Settings Configuration

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

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

Downloaded from www.Manualslib.com manuals search engine

Figure 74 ADVANCED > SYSLOG > Log Settings

SYSLOG

Syslog | Log Settings

System

Syslog	Email	Syslog Name	Description	Interval Time
☐	☐	System Information	A log including the system information will be sent according to specified interval time	60 minutes
☐	☐	System Boot Notice	Once system reboots, the log will be sent	When system reboot
☐	☐	System Manager Activity Information	A log will be sent if system manager (Administrator, Supervisor or Account Manager) login to or logout from the device	When system manager login or logout

Subscriber

Syslog	Email	Syslog Name	Description	Interval Time
☐	☐	Wireless Association Information	A log including wireless users information will be sent according to specified interval time	60 minutes
☐	☐	Logged-in Users	A login users information will be sent according to specified interval time	60 minutes

Proprietary Accounting

Syslog	Email	Syslog Name	Description	Interval Time
☐	☐	Account Created	A log will be sent once after an account is created	When an account is created
☐	☐	Account Activated	A log will be sent once after an account is activated	When an account is activated
☐	☐	Subscriber Trace	A log included subscribers login/logout time would be sent once after subscriber logout	When subscriber logout or idle-timeout
☐	☐	User Agreement	A log would be sent when "user agreement" enabled	When subscriber login

Billing

Syslog	Email	Syslog Name	Description	Interval Time
☐	☐	Billing Log	A log would be sent after a billing log is created	When log created

LAN Devices Management

Syslog	Email	Syslog Name	Description	Interval Time
☐	☐	LAN Devices Information	A log included current LAN Devices Status would be sent according to specified interval time	60 minutes
☐	☐	LAN Devices Alarm	A log would be send if one of the LAN Devices detected result is FAIL	When device fail

Apply

Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

ADVANCED > SYSLOG > 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 ZyXEL Device sends the syslog. If available, enter the number of minutes the ZyXEL Device waits between sending the syslog.
Apply	Click **Apply** to save the settings.

The following table describes the syslog formats.

Table 36 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 the device reboots, when system reboot
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.
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).

Downloaded from www.Manualslib.com manuals search engine

Table 36 Log Formats (continued)

SYSLOG NAME	FORMAT	CREATED
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.
User Agreement	(**Id**, Mac Address) (**User Agreement**, Type, User IP, User MAC) Where: Type: Agree | Do not agree	When "user agreement" is enabled.
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 ZyXEL Device cannot connect to an attached LAN device.

Downloaded from www.Manualslib.com manuals search engine

Table 37 Subscriber Trace Relationship

TYPE	EVENT	TIME LEFT
TimeToFinish	Finished	00:00:00
TimeToFinish	Replenished	00:12:00 to S/Nxxxxxx
TimeToFinish	Deleted	00:12:00
Accumulation	Finished	00:00:00
Accumulation	Replenished	00:12:00 to S/Nxxxxxx
Accumulation	Logout	00:48:00
Accumulation	Idle-Timeout	00:48:00
Accumulation	Deleted	00:48:00
Accumulation	Account Expired	00:48:00
PostPaid	Logout	******
PostPaid	Idle-Timeout	******
PostPaid	Deleted	******
PostPaid	Finished	******
PostPaid	Account Expired	******
Super	Idle-Timeout	******
Super	Deleted	******

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 19
Session Trace

This chapter shows you how to configure the ZyXEL Device's session trace feature.

19.1 Session Trace

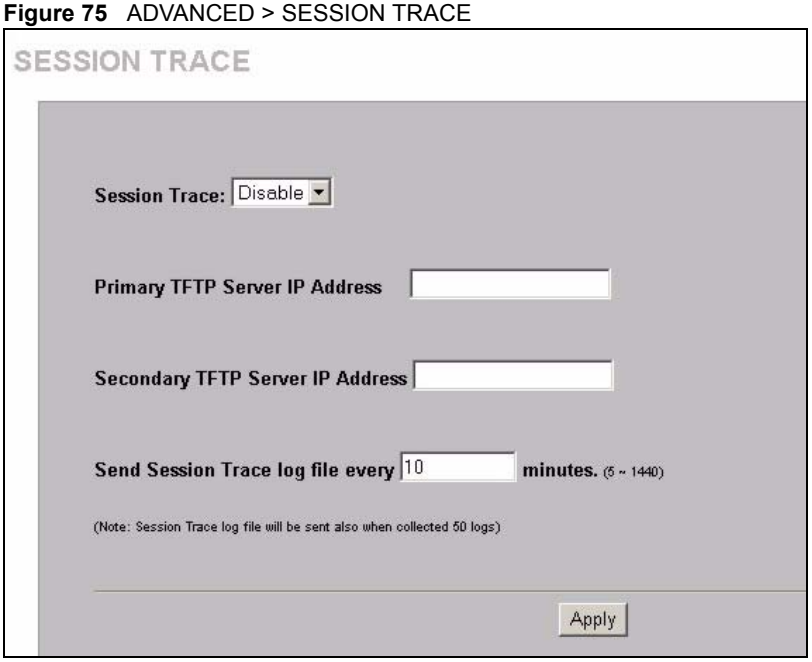
You can set the ZyXEL Device to send session information of subscribers accessing the Internet. The ZyXEL Device records the session information and stores it temporary. Once the session trace information reaches 50 records or the specified time period is reached, the ZyXEL Device sends the session information to the specified TFTP server.

19.2 Session Trace Configuration

Use the **SESSION TRACE** screen to configure to the ZyXEL Device to record details about subscriber Internet access and send logs of the session traces to a TFTP server.

To configure the session trace settings, click **ADVANCED > SESSION TRACE** to display the screen as shown next.

Figure 75 ADVANCED > SESSION TRACE



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

ADVANCED > SESSION TRACE

LABEL	DESCRIPTION
Session Trace	Enable the session trace feature to record the destination IP address, destination port, source IP address, source MAC address and source port of every subscriber session. The ZyXEL Device sends the collected information in a text file to the TFTP server that you specify. Disable the session trace feature to not record and send details about the Internet access activity of your subscribers.
Primary TFTP Server IP Address	Enter the IP address of the first TFTP server in dotted decimal notation.
Secondary TFTP Server IP Address	Enter the IP address of the second TFTP server in dotted decimal notation.
Send Session Trace log file every~ minutes.	Enter the time interval (minutes) for how often you want the ZyXEL Device to sent the session trace log file. **Note:** The ZyXEL Device will also automatically send the log file whenever the log has 50 entries. The ZyXEL Device clears the session trace record after sending a log file.
Apply	Click **Apply** to save the settings.

19.3 Session Trace Filename Convention

The subscriber session information is stored a plain text file with a "txt" filename extension. The general structure of the filename is <hostname>DDMMYYHHMMSS.txt. For example, "MIS221004131543.txt" is the file name of a session information file created at 13:15:43 PM on October 22, 2004 on a ZyXEL Device with a hostname of "MIS".

You can view the subscriber session trace information using any text editor. The following figure shows an example of the session information file the ZyXEL Device sends to a TFTP server.

Figure 76 Session Trace Information Example

```
Host Name User Name   Date    SourceIP      SourceMac    SourcePort DestIP        DestPor
MyDevice 79mv9r33  16Aug05165501 192.168.1.2   000FFE1E4AE0 2101   66.102.7.147   80
MyDevice 79mv9r33  16Aug05165517 192.168.1.2   000FFE1E4AE0 2104   168.95.1.1     53
MyDevice 79mv9r33  16Aug05165517 192.168.1.2   000FFE1E4AE0 2105   69.44.58.78    80
```


Downloaded from www.Manualslib.com manuals search engine

The following table describes the fields in a session information file.

Table 38 Session Trace File Fields

FIELD	DESCRIPTION
Host Name	This is the host (or system) name of the ZyXEL Device.
User Name	This is the subscriber account username. This field is empty if you disable authentication in the Authentication screen (see Chapter 6, "Authentication," on page 69 for more information).
Date	This is the date and time the ZyXEL Device creates a session trace record.
SourceIP	This is the IP address of the subscriber.
SourceMac	This is the MAC address of the subscriber's computer.
SourcePort	This is the source port number of the subscriber.
DestIP	This is the destination IP address the subscriber accesses.
DestPort	This is the destination port number for this session.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 20
Bandwidth

This chapter shows you how to configure the ZyXEL Device's bandwidth management feature.

20.1 Bandwidth

You can set the ZyXEL Device to limit the amount of bandwidth each user can use. This prevents one user from consuming a disproportionately large amount of bandwidth and helps ensure that every user gets their fair share. If there is a lot of unused bandwidth, however, this feature is not necessary and slows down users who could use the extra bandwidth to upload or download large amounts of information more quickly.

The ZyXEL Device separates bandwidth into upstream bandwidth and downstream bandwidth. Upstream bandwidth is used when users send information to the WAN, and downstream bandwidth is used when users receive information from the WAN. This distinction is helpful when you might want to set limits one way but not the other. For example, if your users download a lot of MP3 files, you might set a limit on downstream bandwidth but not set a limit on upstream bandwidth. In other situations, however, you might put the same limit on upstream and downstream bandwidth.

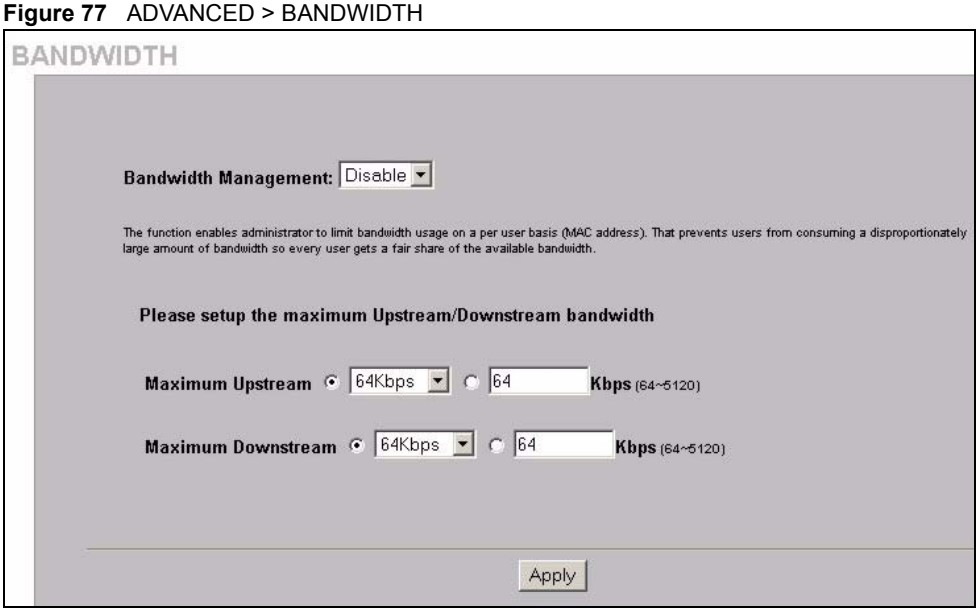
20.2 Bandwidth Configuration

Use the **BANDWIDTH** screen to configure to the ZyXEL Device to limit the amount of upstream and downstream bandwidth each user can use.

To configure the bandwidth settings, click **ADVANCED > BANDWIDTH** to display the screen shown next.

Downloaded from www.Manualslib.com manuals search engine

Figure 77 ADVANCED > BANDWIDTH



The following table describes the labels in this screen.

Table 39 ADVANCED > BANDWIDTH

LABEL	DESCRIPTION
Bandwidth Management	Select **Enable** to turn on bandwidth management. If you select **Disable**, each user gets as much bandwidth as possible until the available bandwidth is gone.
Maximum Upstream	Select the maximum amount of upstream (outbound) bandwidth or enter a specific amount of bandwidth in Kbps that any user can have.
Maximum Downstream	Select the maximum amount of downstream (inbound) bandwidth or enter a specific amount of bandwidth in Kbps that any user can have.
Apply	Click **Apply** to save the settings.

Downloaded from www.Manualslib.com manuals search engine

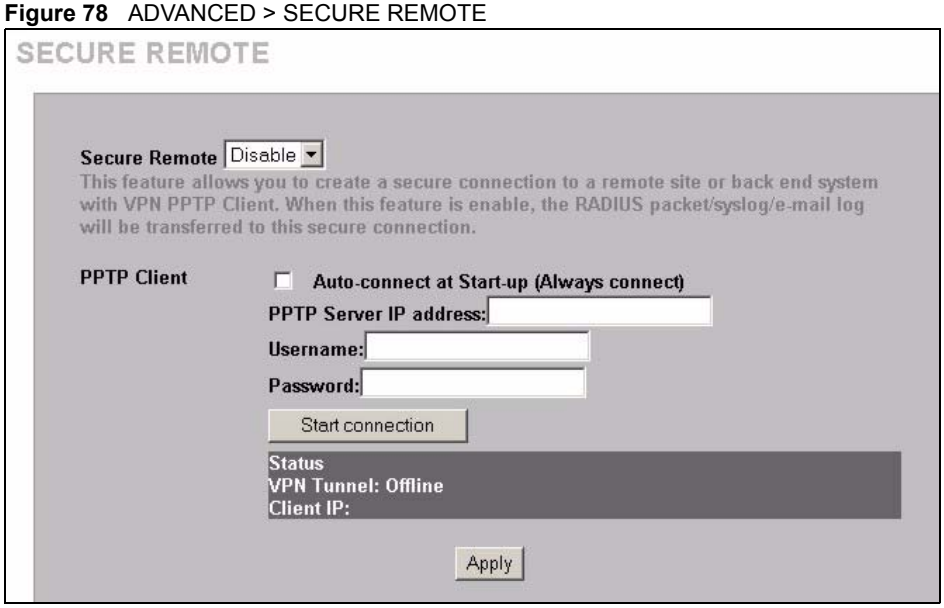
CHAPTER 21
Secure Remote

This chapter shows you how to configure settings to use the ZyXEL Device's VPN PPTP client for a secure connection to a remote site or back end system.

21.1 Secure Remote Configuration

Click **ADVANCED > SECURE REMOTE** to open the following screen. Configure this screen to have the ZyXEL Device send RADIUS packets, syslogs and log e-mails through a PPTP VPN tunnel.

Figure 78 ADVANCED > SECURE REMOTE



The following table describes the labels in this screen.

Table 40 ADVANCED > SECURE REMOTE

LABEL	DESCRIPTION
Secure Remote	Select **Enable** to have the ZyXEL Device send RADIUS packets, syslogs and log e-mails through a PPTP VPN tunnel.
Auto-connect at Start-up (Always connect)	Turn this on to have the ZyXEL Device automatically establish this connection after it turns on.
PPTP Server IP address	Enter the IP address of the PPTP server to which the ZyXEL Device will make the secure connection.

Downloaded from www.Manualslib.com manuals search engine

Table 40 ADVANCED > SECURE REMOTE (continued)

LABEL	DESCRIPTION
Username	Enter the user name exactly as it was provided by the ISP or network administrator. The user name can be up to 80 alphanumeric characters and is case-sensitive.
Password	Enter the password exactly as it was provided by the ISP or network administrator. The password can be up to 80 alphanumeric characters and is case-sensitive.
Start/Stop Connection	Click this button to initiate or cancel the PPTP connection.
Status	
VPN Tunnel	This field displays whether or not the PPTP connection is currently up.
Client IP	This is the IP address that the PPTP server assigned to the ZyXEL Device for the VPN connection.
Apply	Click **Apply** to save the settings.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 22
Account Generator

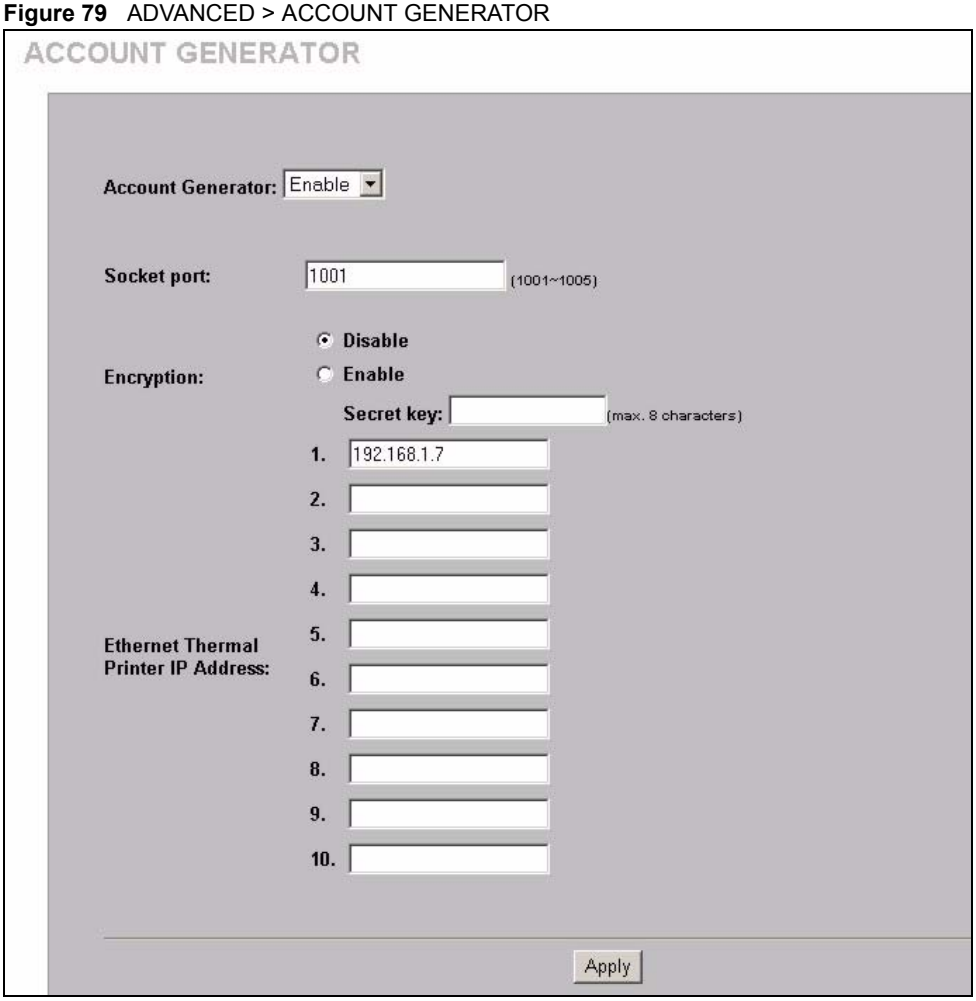
This chapter shows you how to configure settings for the account generator (also known as the statement printer or "exclusive printer").

22.1 Account Generator Configuration

Click **ADVANCED > ACCOUNT GENERATOR** to open the following screen. Use this screen to configure the settings for using the ZyXEL Device with one or more account generators (statement printers).

Downloaded from www.Manualslib.com manuals search engine

Figure 79 ADVANCED > ACCOUNT GENERATOR



The following table describes the labels in this screen.

Table 41 ADVANCED > ACCOUNT GENERATOR

LABEL	DESCRIPTION
Account Generator	Select **Enable** to use an account generator (statement printer) to generate subscriber accounts and print subscriber statements.
Socket port	This is the port number that your account generator (statement printer) uses. If you change this, make sure you also change it in the printer, see the printer's user's guide for how to do this.
Encryption	Turn on the encryption to encode the data that the ZyXEL Device sends to the statement printer(s). When you use the encryption, the data is unreadable to anyone that does not know the secret key. This protects against people stealing account information or creating illegitimate accounts. To use encryption, you must also configure the secret key in the following field and on the statement printer(s).

Downloaded from www.Manualslib.com manuals search engine

Table 41 ADVANCED > ACCOUNT GENERATOR (continued)

LABEL	DESCRIPTION
Secret key	When you use encryption, enter a code here. You can use up to 8 ASCII characters. You must also configure the same code as the secret key on the statement printer(s).
Ethernet Thermal Printer IP Address	This is the IP address that a statement printer uses. If you change this, make sure you also change it in the printer, see the printer's user's guide for how to do this. You can use multiple statement printers with the ZyXEL Device. Each device on your network (including statement printers) must have a unique IP address. The port number however can be the same for more than one device.
Apply	Click **Apply** to save the settings.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 23
Wireless LAN

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

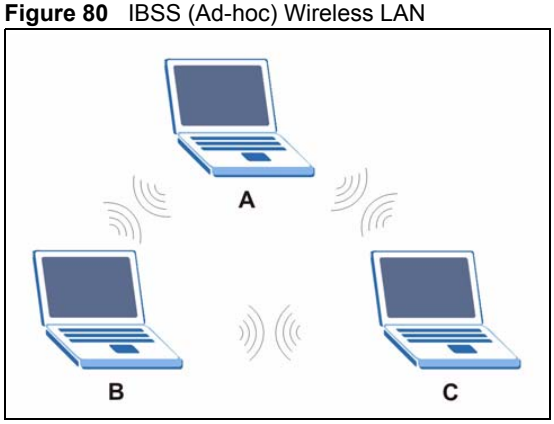
23.1 Wireless LAN Overview

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

23.1.1 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 80 IBSS (Ad-hoc) Wireless LAN



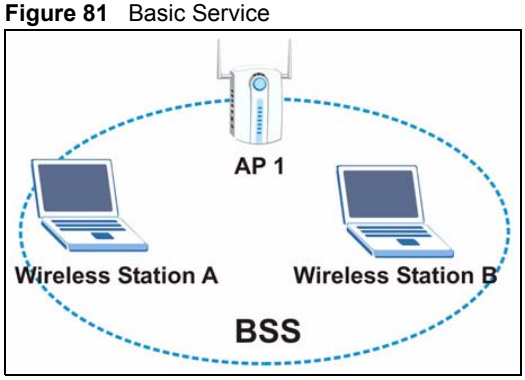
23.1.2 BSS

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.

Downloaded from www.Manualslib.com manuals search engine

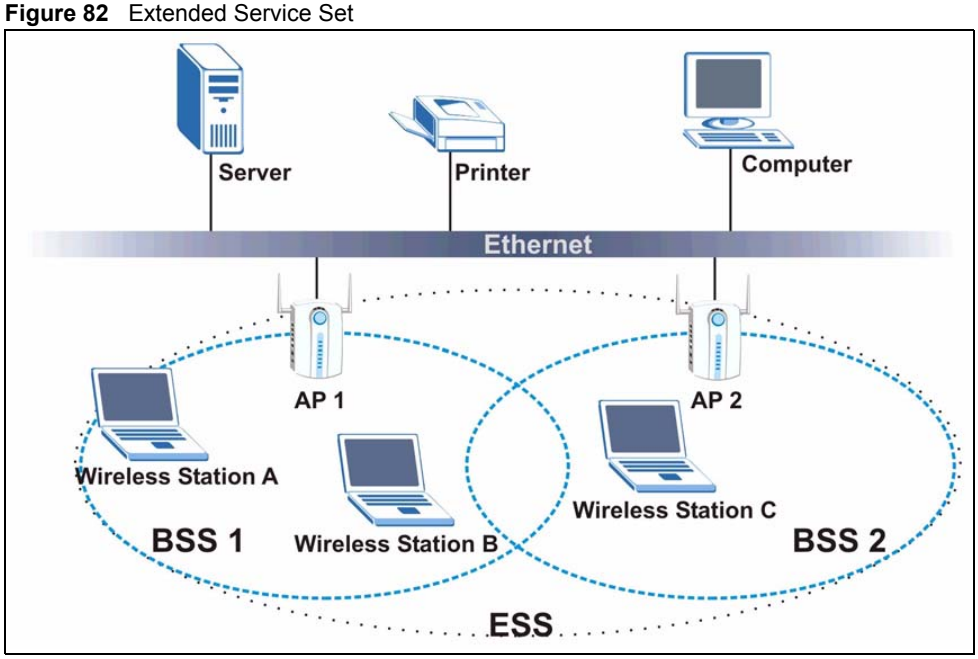
Figure 81 Basic Service



23.1.3 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 82 Extended Service Set



23.2 Wireless LAN Basics

This section provides background information on Wireless LAN features.

Downloaded from www.Manualslib.com manuals search engine

23.2.1 Wireless Standards

The ZyXEL Device complies with the IEEE 802.11g wireless standard and is also fully compatible with the 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g device (and vice versa) at 11 Mbps or lower depending on range. The IEEE 802.11b data rate and corresponding modulation techniques are shown in the table below. The modulation technique defines how bits are encoded onto radio waves.

Table 42 IEEE 802.11b Data Rates and Modulation

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)

IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 43 IEEE 802.11g Data Rates and Modulation

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

Note: The ZyXEL Device 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.

23.2.2 Wireless LAN Coverage

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

Table 44 Wireless LAN Coverage

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

23.2.3 Channel

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

Downloaded from www.Manualslib.com manuals search engine

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.

23.2.4 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption. WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You cannot use the ZyXEL Device's built-in authentication for WPA authentication purposes since the built-in authentication uses EAP-MD5, which cannot be used to generate keys.

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

23.2.5 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.

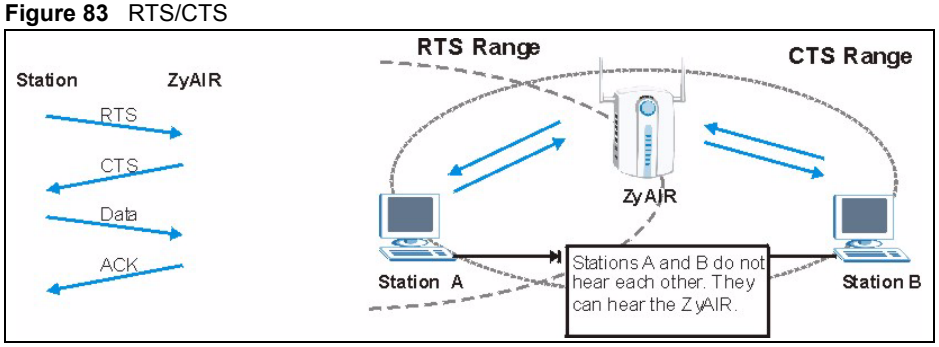
WEP degrades performance.

23.2.6 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.

Downloaded from www.Manualslib.com manuals search engine

Figure 83 RTS/CTS



When station A sends data to the ZyXEL Device, 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.

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

23.2.7 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 ZyXEL Device will fragment the packet into smaller data frames.

Downloaded from www.Manualslib.com manuals search engine

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.

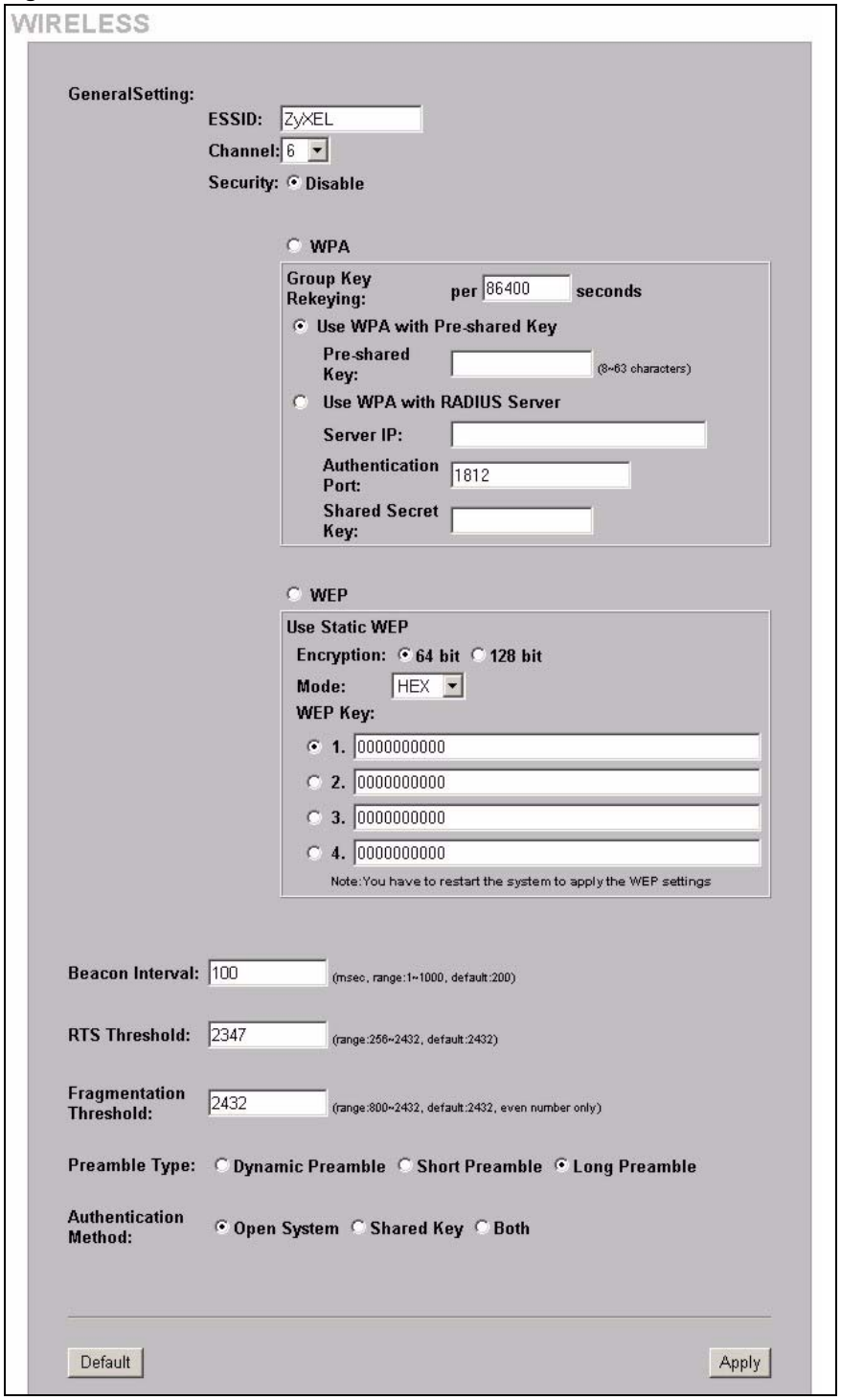
23.3 Wireless LAN Setup

Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device'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 ZyXEL Device's new settings.

Click **ADVANCED > WIRELESS** to open this screen.

Downloaded from www.Manualslib.com manuals search engine

Figure 84 ADVANCED > WIRELESS



Downloaded from www.Manualslib.com manuals search engine

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

Table 45 ADVANCED > 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 ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device'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 ZyXEL Device's new settings.
Channel	Select a channel from the drop-down list box depending on your particular region.
Security	Select **Disable** to allow wireless devices to communicate with the ZyXEL Device without any data encryption. Select **WPA** (Wi-Fi Protected Access) to have the ZyXEL Device perform user authentication and data encryption. WPA's data encryption is stronger than WEP. Select **WEP** (Wired Equivalent Privacy to have the ZyXEL Device encrypt data frames before transmitting them over the wireless network. Select the check box to enable WEP data encryption. Then configure the WEP keys.
WPA	
Group Key Rekeying	The **Group Key Rekeying** field sets how often the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The default is 8,600 seconds.
Use WPA with Pre-shared Key	Select this radio button to use a pre-shared key for WPA. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Use WPA with RADIUS Server	Select this radio button to use a RADIUS server to authenticate the wireless clients.
Server IP/ Domain	Enter the external authentication server's IP address (in dotted decimal notation) or domain name.
Authentication Port	You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key is not sent over the network. This key must be the same on the external authentication server and the ZyXEL Device.
WEP	
Encryption	Select **64-bit** or **128-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.

Downloaded from www.Manualslib.com manuals search engine

Table 45 ADVANCED > WIRELESS (continued)

LABEL	DESCRIPTION
WEP Key 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" (for example 11AA22BB33) for HEX key type or Enter 5 printable ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example 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. **Note:** The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. ASCII WEP keys are case sensitive.
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.
Preamble Type	Preamble is used to signal that data is coming to the receiver. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble. Select **Long Preamble** if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks. Select **Short Preamble** if you are sure the wireless adapters support it, and to provide more efficient communications.
Authentication Method	Select **Open System** to allow any device to authenticate and then attempt to communicate with the ZyXEL Device. Using open authentication, any wireless device can authenticate with the ZyXEL Device, but the device can only communicate if its WEP keys match the ZyXEL Device. Devices not using WEP do not attempt to authenticate with a ZyXEL Device that is using WEP. Open authentication does not rely on a RADIUS server on your network. Select **Shared Key** to have the ZyXEL Device use shared key authentication. The ZyXEL Device sends an unencrypted challenge text string to any device attempting to communicate with the ZyXEL Device. The device-requesting authentication encrypts the challenge text and sends it back to the ZyXEL Device. If the challenge text is encrypted correctly, the ZyXEL Device allows the requesting device to authenticate. However, both the unencrypted challenge and the encrypted challenge can be monitored; thus leaving the ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

Table 45 ADVANCED > WIRELESS (continued)

LABEL	DESCRIPTION
Default	Click this button to load the factory default wireless LAN settings.
Apply	Click **Apply** to save the settings.

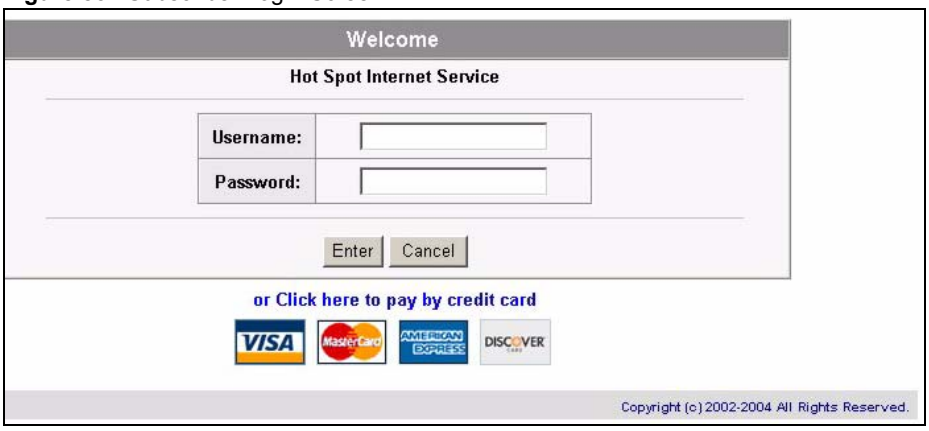
Downloaded from www.Manualslib.com manuals search engine

CHAPTER 24
Subscriber Login

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

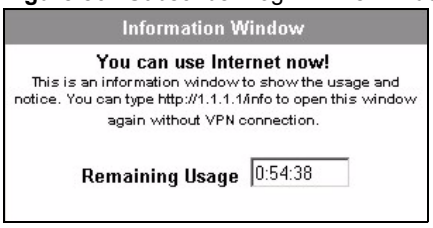
If user authentication is activated, the login screen displays prompting you to enter the user name and password. A standard subscriber login screen (with the credit card function) is shown in the figure below.

Figure 85 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.

Figure 86 Subscriber Login: Time Window



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 25
Report Printing Using the SP-200E

This appendix shows you how to print reports using the SP-200E. See the SP-200E User's Guide for details on how to set up the SP-200E.

25.1 Reports Overview

The SP-200E allows you to print status reports about the subscriber accounts and general ZyAIR system information. Simply press a key combination on the SP-200E to print a report instantly without accessing the web configurator.

The following lists the reports that you can print using the SP-200E.

- Daily account summary
- Monthly account summary
- System status
- Network statistics

25.2 Key Combinations

The following table lists the key combination to print each report.

Note: You must press the key combination on the SP-200E within five seconds to print.

Table 46 Report Printing Key Combinations

REPORT TYPE	KEY COMBINATION
Daily Account Summary	A B C A A
Monthly Account Summary	A B C B B
System Status	A B C C C
Network Statistics	A B C A B

The following sections describe each report printout in detail.

Downloaded from www.Manualslib.com manuals search engine

25.3 Daily Account Summary

The daily account report lists the accounts printed during the current day, the current day's total number of accounts and the total charge. It covers the accounts that have been printed during the current day starting from midnight (not the past 24 hours). For example, if you press the daily account key combination on 2005/8/1 at 20:00:00, the daily account report includes the accounts created on 2005/8/1 between 00:00:01 and 19:59:59.

Key combination: A B C A A

The following figure shows an example. "B" stands for the button that was pressed to generate the account. "UN" stands for the units of Internet access that were purchased.

Figure 87 Daily Account Example

```
          Daily Account
----------------------------
           2005/8/1

S/N   Username  B  UN  Price
----------------------------
 000002 p2m6pf52 1  1   1.00
 000003 s4pcms28 1  2   2.00
----------------------------
      TOTAL ACCOUNTS: 2
     TOTAL PRICE: $ 3.00
----------------------------
      2005/8/1  20:00:11
          ---End---
```

25.4 Monthly Account Summary

The monthly account report lists the accounts printed during the current month, the current month's total number of accounts and the total charge. It covers the accounts that have been printed during the current month starting from midnight of the first day of the current month (not the past one month period). For example, if you press the monthly account key combination on 2005/8/17 at 20:00:00, the monthly account report includes the accounts created from 2005/8/1 at 00:00:01 to 2005/8/17 at 19:59:59.

Key combination: A B C B B

The following figure shows an example. "B" stands for the button that was pressed to generate the account. "UN" stands for the units of Internet access that were purchased.

Downloaded from www.Manualslib.com manuals search engine

Figure 88 Monthly Account Example

```
        Monthly Account
----------------------------
           2005/8/1

S/N   Username  B  UN  Price
----------------------------
 000002 p2m6pf52 1  1   1.00
 000003 s4pcms28 1  2   2.00
 000004 7ufm7z22 2  1   2.00
 000005 qm5fxn95 3  2   6.00

----------------------------
      TOTAL ACCOUNTS: 4
    TOTAL PRICE: $ 11.00
----------------------------
     2005/8/1  20:00:11
          ---End---
```

25.5 Account Report Notes

The daily or monthly account report holds up to 2000 entries. If there are more than 2000 accounts created in the same month or same day, the account report's calculations only include the latest 2000.

For example, if 2030 accounts (each priced at $1) have been created from 2005/7/1 00:00:00 to 2005/7/31 19:59:59, the monthly account report includes the latest 2000 accounts, so the total would be $2,000 instead of $2,030.

Use the **SYSTEM STATUS > ACCOUNT LOG** screen to see the accounts generated on another day or month (up to 2000 entries total).

25.6 System Status

This report shows the current system information such as the host name and WAN IP address.

Key combination: A B C C C

The following figure shows an example.

Downloaded from www.Manualslib.com manuals search engine

Figure 89 System Status Example

```
        System Status
----------------------------
      ITEM DESCRIPTION
----------------------------
      WAST ESTABLISHED
        WSTA Success
    SYST 02D:02H:42M:46S
----------------------------
        HOST MyDevice
     FRMW v1.00(ZB.2)CO
            WFRM
          BTRM 1.01
            LOCA
   WAMA 00-90-0E-00-4A-29
   LAMA 00-90-0E-00-4A-28
          WATP DHCP
      WAIP 172.21.2.67
      WASM 255.255.0.0
     WAGW 172.21.0.254
      PDNS 172.20.0.63
      SDNS 172.20.0.27
      DHCP DHCP SERVER
       DHSP 10.59.1.2
      DHEP 10.59.1.254
          DHLT 1440
        EMAIL /PORT25
----------------------------
     2004/10/28 11:24:42
          ---End---
```

The following table describes the labels in this report.

Table 47 System Status

LABEL	DESCRIPTION
WAST	This field displays the WAN connection status.
WSTA	This field displays the status of the ZyAIR's wireless LAN.
SYST	This field displays the time since the system was last restarted.
HOST	This field displays the description name of the ZyAIR for identification purposes.
FRMW	This field displays the version of the firmware on the ZyAIR.
WFRM	This field displays the version of the (internal) wireless adapter firmware on the ZyAIR.
BTRM	This field displays the version of the bootrom.
WAMA	This field displays the MAC address of the ZyAIR on the WAN.
LAMA	This field displays the MAC address of the ZyAIR on the LAN.
WATP	This field displays the mode of the WAN port.
WAIP	This field displays the IP address of the WAN port on the ZyAIR.

Downloaded from www.Manualslib.com manuals search engine

Table 47 System Status (continued)

LABEL	DESCRIPTION
WASM	This field displays the subnet mask of the WAN port on the ZyAIR.
WAGW	This field displays the IP address of the default gateway of the WAN port on the ZyAIR.
PDNS	This field displays the IP address of the primary DNS server.
SDNS	This field displays the IP address of the secondary DNS server.
DHCP	This field displays the DHCP mode (**DHCP Server**, **Relay** or **DHCP Disable**) on the LAN.
DHSP	If the **DHCP** field is **DHCP Server**, this field displays the first of the continuous addresses in the IP address pool. If the **DHCP** field is **DHCP Relay**, this field displays the DHCP server IP address.
DHEP	This field is visible when the **DHCP** is **DHCP Server**. This field displays the end of the continuous addresses in the IP address pool.
DHLT	This field is visible when the **DHCP** is **DHCP Server**. This field displays the time (in minutes) a DHCP client is allowed to use an assigned IP address.
EMAIL	The field displays e-mail server port number.
SSID	This field displays the ZyAIR's Extended Service Set IDentity.
WCHA	This field displays the channel that the ZyAIR is using.
WSEC	This field displays whether the ZyAIR's wireless security is turned on or off.

25.7 Network Statistics

This report shows the network statistics on the ZyAIR.

Key combination: A B C A B

The following figure shows an example.

Downloaded from www.Manualslib.com manuals search engine

Figure 90 Network Statistics Example

```
          Network
----------------------------
      ITEM DESCRIPTION
----------------------------
      WAST ESTABLISHED
        WSTA Success
    SYST 02D:02H:42M:46S
----------------------------
          WATD 37
         WARD 4816
          WATE 0
          WARE 0
         LATD 1768
         LARD 4616
          LATE 0
          LARE 0
----------------------------
     2004/10/28 15:24:42
         ---End---
```

The following table describes the labels in this report.

Table 48 Network Statistics

LABEL	DESCRIPTION
WAST	This field displays the WAN connection status.
WSTA	This field displays the wireless LAN status.
SYST	This field displays the time since the system was last restarted.
WATD	This field displays the number of packets transmitted on the WAN.
WARD	This field displays the number of packets received on the WAN.
WATE	This field displays the number of error packets transmitted on the WAN.
WARE	This field displays the number of error packets received on the WAN.
LATD	This field displays the number of packets transmitted on the LAN.
LARD	This field displays the number of packets received on the LAN.
LATE	This field displays the number of error packets transmitted on the LAN.
LARE	This field displays the number of error packets received on the LAN.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 26
System Status

This chapter describes the screens under SYSTEM STATUS.

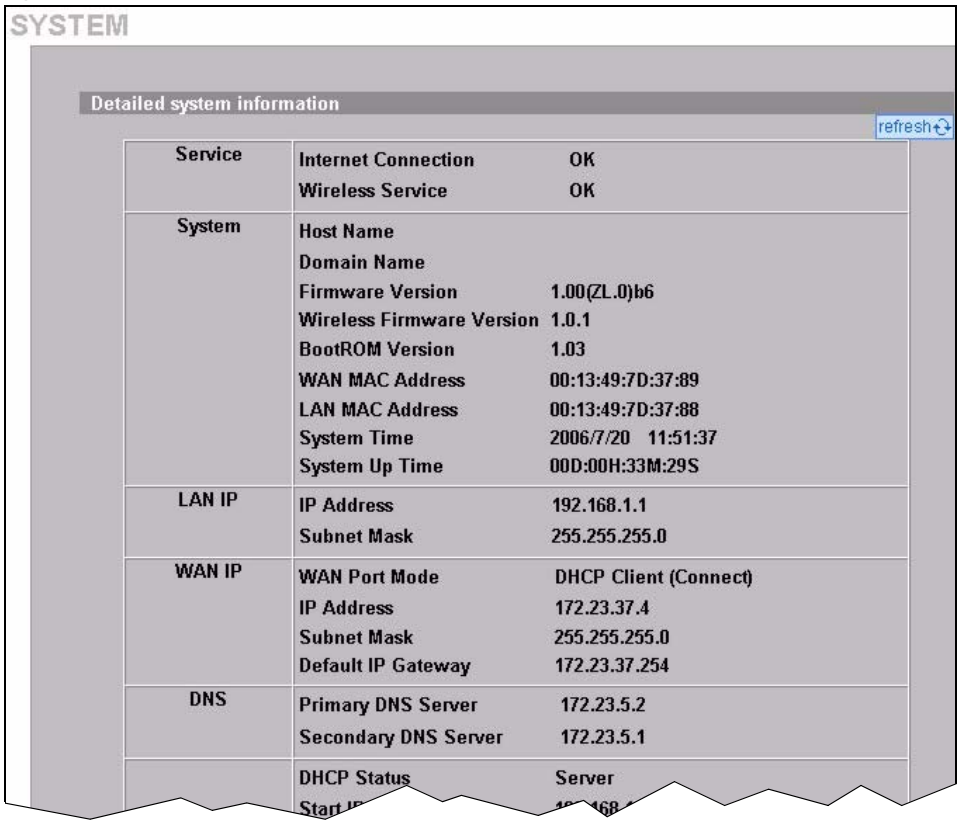
26.1 About System Status

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

26.2 View System Information

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

Figure 91 SYSTEM STATUS > SYSTEM



Downloaded from www.Manualslib.com manuals search engine

	...nary DNS Server	172.[illegible].1	
DHCP	DHCP Status	Server	
	Start IP Address	192.168.1.32	
	End IP Address	192.168.1.231	
	Lease Time	300	
Wireless	ESSID	ZyXEL	
	Channel	6	
	Encryption	Disable	
E-mail Redirection			
Network Traffic	WAN Traffic	Tx Data:	18647
		Rx Data:	275088
		Tx Error:	0
		Rx Error:	0
	LAN Traffic	Tx Data:	377230
		Rx Data:	165438
		Tx Error:	0
		Rx Error:	0
	Wireless Traffic	Tx Data:	1
		Rx Data:	15938
		Tx Error:	0
		Rx Error:	0
Location Information	Location Name		
	Address		
	City		
	State / Province		
	ZIP / Postal Code		
	Country		
	Contact Name		
	Contact Telephone		
	Contact FAX		
	Contact Email		
SSL Certificate	Country	00	
	State	Local State	
	Local City	Local City	
	Organization	Local Group	
	Organization Unit	Local Host	
	Common Name	1.1.1.1	
	Email Address	mail@1.1.1.1	

Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 49 SYSTEM STATUS > SYSTEM

LABEL	DESCRIPTION
Service	
Internet Connection	This field displays the status of the ZyXEL Device's connection to the Internet.
Wireless Service	This field displays the status of the ZyXEL Device's wireless LAN.
System	
Host Name	This field displays the description name of the ZyXEL Device for identification purposes.
Domain Name	This field displays the domain name of the ZyXEL Device.
Firmware Version	This field displays the version of the firmware on the ZyXEL Device.
Wireless Firmware Version	This field displays the version of the wireless features on the ZyXEL Device.
Bootrom Version	This field displays the version of the bootbase in the ZyXEL Device.
WAN MAC Address	This field displays the MAC address of the ZyXEL Device on the WAN.
LAN MAC Address	This field displays the MAC address of the ZyXEL Device on the LAN.
System Time	This field displays the ZyXEL Device's current time.
System Up Time	This field displays the how long the ZyXEL Device has been operating since it was last started.
LAN IP	
IP Address	This field displays the IP address of the LAN port on the ZyXEL Device.
Subnet Mask	This field displays the subnet mask of the LAN port on the ZyXEL Device.
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 ZyXEL Device.
Subnet Mask	This field displays the subnet mask of the WAN port on the ZyXEL Device.
Default IP Gateway	This field displays the IP address of the default gateway of the WAN port on the ZyXEL Device.
DNS	
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 ZyXEL Device's Extended Service Set IDentity.

Downloaded from www.Manualslib.com manuals search engine

Table 49 SYSTEM STATUS > SYSTEM (continued)

LABEL	DESCRIPTION
Channel	This field displays the channel that the ZyXEL Device is using.
Encryption	This field displays the type of data encryption that the ZyXEL Device is using. **WEP** displays if the ZyXEL Device is using WEP data encryption. **WPA** displays if ZyXEL Device is using WPA data encryption. **Disable** displays if the ZyXEL Device is not using data encryption.
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 ZyXEL Device's WAN connection.
LAN Traffic	This field displays traffic statistics for the ZyXEL Device's LAN connection.
Wireless Traffic	This field displays traffic statistics for the ZyXEL Device's wireless LAN connection.
Location Information	
Location Name	This field displays the device's geographical location.
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.

26.3 Account List

Refer to Section 8.5 on page 85 for an example and explanation of the ACCOUNT LIST screen.

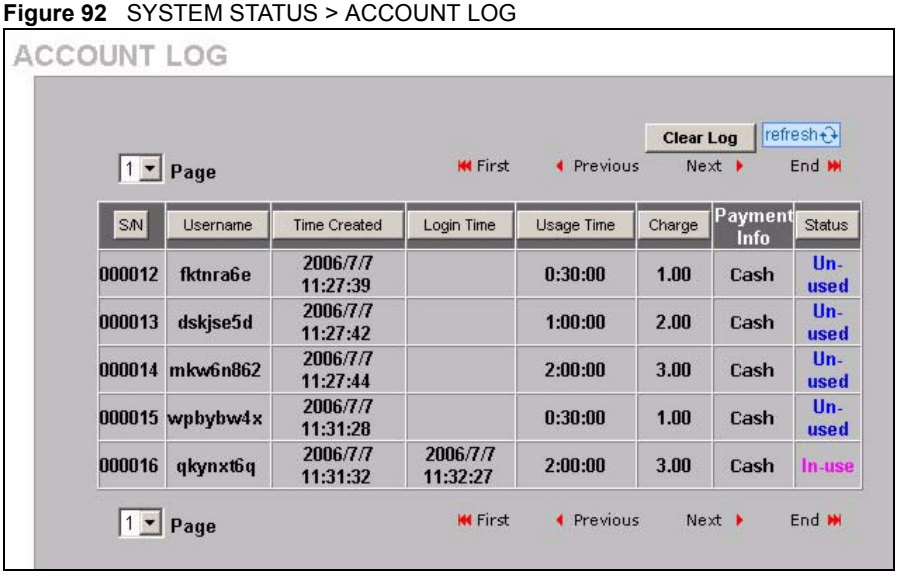
Downloaded from www.Manualslib.com manuals search engine

26.4 Account Log

This screen displays information on the ZyXEL Device's subscriber account logs.

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

Figure 92 SYSTEM STATUS > ACCOUNT LOG



The following table describes the labels in this screen.

Table 50 SYSTEM STATUS > ACCOUNT LOG

LABEL	DESCRIPTION
Clear Log	Click **Clear Log** to remove all of the log entries from the ZyXEL Device'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.
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.

Downloaded from www.Manualslib.com manuals search engine

Table 50 SYSTEM STATUS > ACCOUNT LOG (continued)

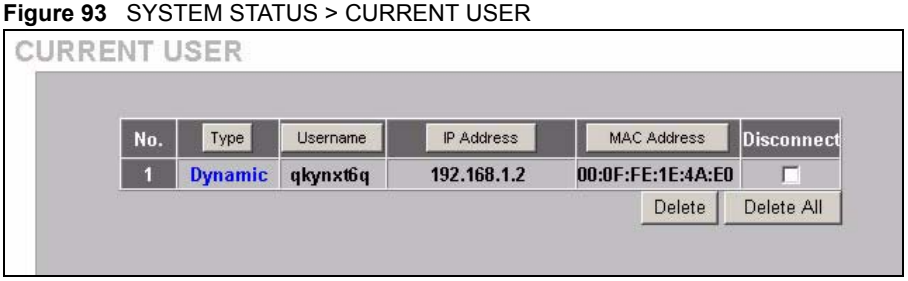
LABEL	DESCRIPTION
Status	This field displays **IN-Used** when the account is currently in use. Otherwise it displays **UN-Used**. This field displays **Finished** when a subscriber uses up the time allocated to an account. This field displays **Expired** when a subscriber's account has reached expiration. 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.

26.5 Current Users

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

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

Figure 93 SYSTEM STATUS > CURRENT USER



The following table describes the labels in this screen.

Table 51 SYSTEM STATUS > 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.
Username	This field is displayed only if any subscribers are using the system. This field displays the username currently used by the account.
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.

Downloaded from www.Manualslib.com manuals search engine

Table 51 SYSTEM STATUS > CURRENT USER (continued)

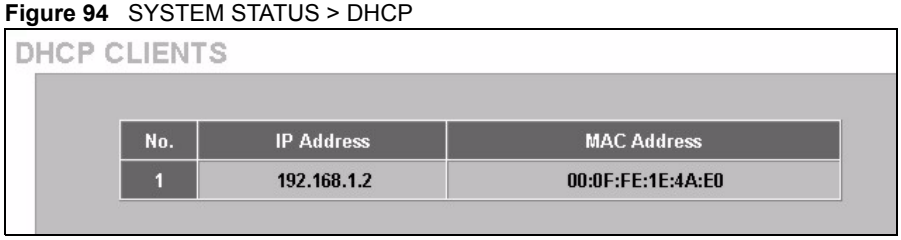
LABEL	DESCRIPTION
Disconnect	This field is displayed only if any subscribers are using the system. Select this(ese) check box(es) and click **Delete** to terminate the selected subscriber connection.
Delete All	Click this button to terminate all subscriber connections.

26.6 DHCP Clients

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

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

Figure 94 SYSTEM STATUS > DHCP



The following table describes the labels in this screen.

Table 52 SYSTEM STATUS > DHCP

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

26.7 Session List

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

Downloaded from www.Manualslib.com manuals search engine

Figure 95 SYSTEM STATUS > Session List

SESSION LIST

1 Page First Previous Next End

No.	TCP/UDP	Client IP	Client Port	Port Fake	Remote IP	Remote Port	Idle
1	UDP	192.168.1.2	1828	50045	172.22.0.3	427	25
2	TCP	192.168.1.2	1970	50010	172.23.5.19	445	51
3	UDP	192.168.1.2	1994	50014	168.95.1.1	53	25
4	UDP	192.168.1.2	1997	50017	168.95.1.1	53	25
5	UDP	192.168.1.2	1998	50018	168.95.1.1	53	25
6	UDP	192.168.1.2	2002	50022	168.95.1.1	53	25
7	UDP	192.168.1.2	2003	50023	168.95.1.1	53	25
8	UDP	192.168.1.2	2005	50025	168.95.1.1	53	25
9	TCP	192.168.1.2	2006	50026	64.86.142.112	80	25
10	TCP	192.168.1.2	2007	50027	64.86.142.112	80	25
11	TCP	192.168.1.2	2009	50029	64.154.81.197	80	25
12	UDP	192.168.1.2	2012	50032	168.95.1.1	53	25
13	UDP	192.168.1.2	2015	50035	168.95.1.1	53	25
14	TCP	192.168.1.2	2016	50036	64.233.167.147	80	25
15	UDP	192.168.1.2	2017	50037	168.95.1.1	53	25
16	TCP	192.168.1.2	2018	50038	209.133.56.106	80	25
17	UDP	192.168.1.2	2019	50039	168.95.1.1	53	25

1 Page First Previous Next End

The following table describes the fields in this screen.

Table 53 SYSTEM STATUS > 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**).
Client IP	This field displays the IP address of the client computer.
Client Port	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 ZyXEL Device 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 ZyXEL Device automatically times out idle TCP sessions after 5 minutes (300 seconds). The ZyXEL Device automatically times out idle UDP sessions after 1 minute (60 seconds).

Downloaded from www.Manualslib.com manuals search engine

26.8 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 > LAN DEVICES** to display the screen as shown next. This screen automatically updates every minute.

Figure 96 SYSTEM STATUS > LAN DEVICES

LAN DEVICES

NO.	Device Name	Status	Virtual Port (60001~60050)	Device IP Address	Device Server Port	Device MAC Address	Application	Interface
1	AP	Fail	60001	10.59.1.2	80	00:AD:C5:01:23:45	TCP	Wired
2	Switch	Fail	60002	10.59.1.3	80	00:00:1C:01:01:6C	TCP	Wired

The following table describes the labels in this screen.

Table 54 SYSTEM STATUS > 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**.
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 ZyXEL Device the LAN device is connected.

26.8.1 Accessing a LAN Device

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

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

Downloaded from www.Manualslib.com manuals search engine

- You have set up the virtual port mapping to the LAN device server port in the **ADVANCED > LAN DEVICES** screen.
- The LAN device status is **OK** in the **SYSTEM STATUS > LAN DEVICES** screen.

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

1. To access the LAN device through the web configurator, open the **SYSTEM STATUS > LAN DEVICES** screen and click the device name. A new Internet browser should display showing the login screen of the LAN device management interface.
2. To directly access the LAN device, enter the WAN IP address of your ZyXEL Device 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 ZyXEL Device. The login screen of the LAN device management interface should display.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 27
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.

27.1 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 ZyXEL Device, 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 ZyXEL Device.

27.2 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.

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

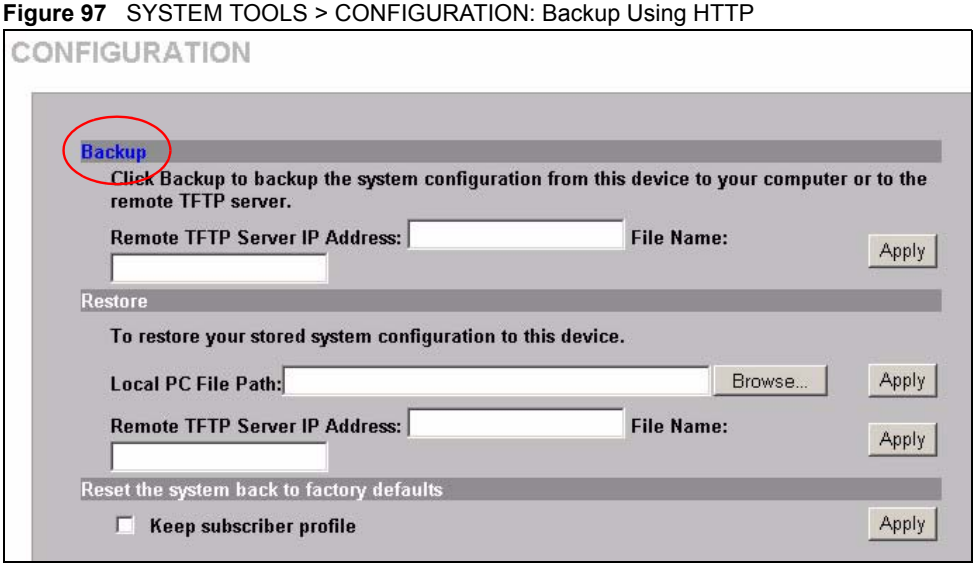
27.2.1 Backup Configuration Using HTTP

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

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

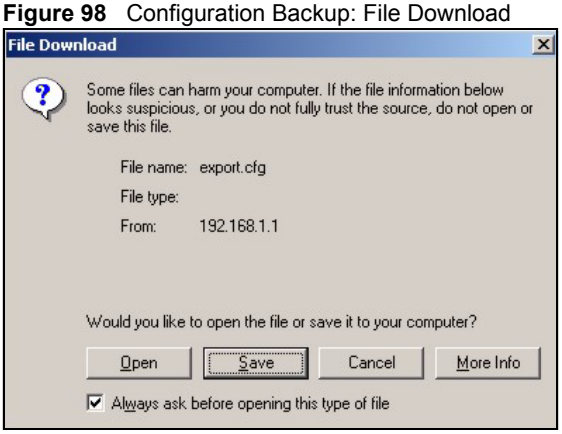
Downloaded from www.Manualslib.com manuals search engine

Figure 97 SYSTEM TOOLS > CONFIGURATION: Backup Using HTTP



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

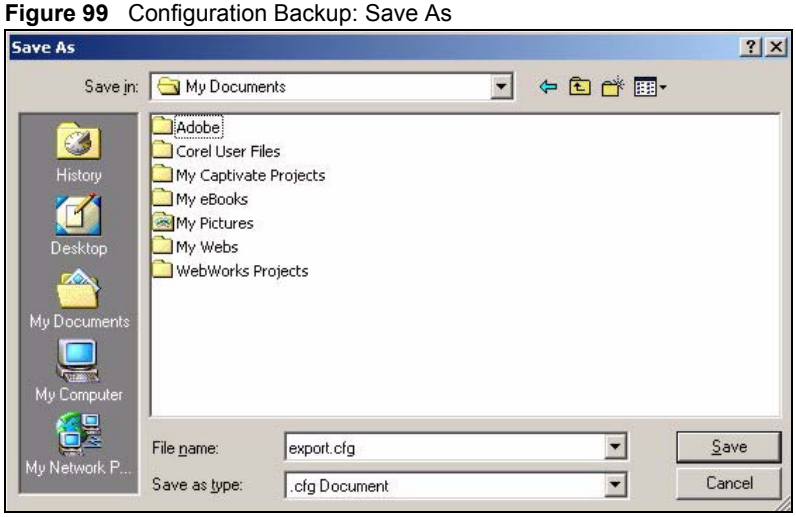
Figure 98 Configuration Backup: File Download



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

Downloaded from www.Manualslib.com manuals search engine

Figure 99 Configuration Backup: Save As



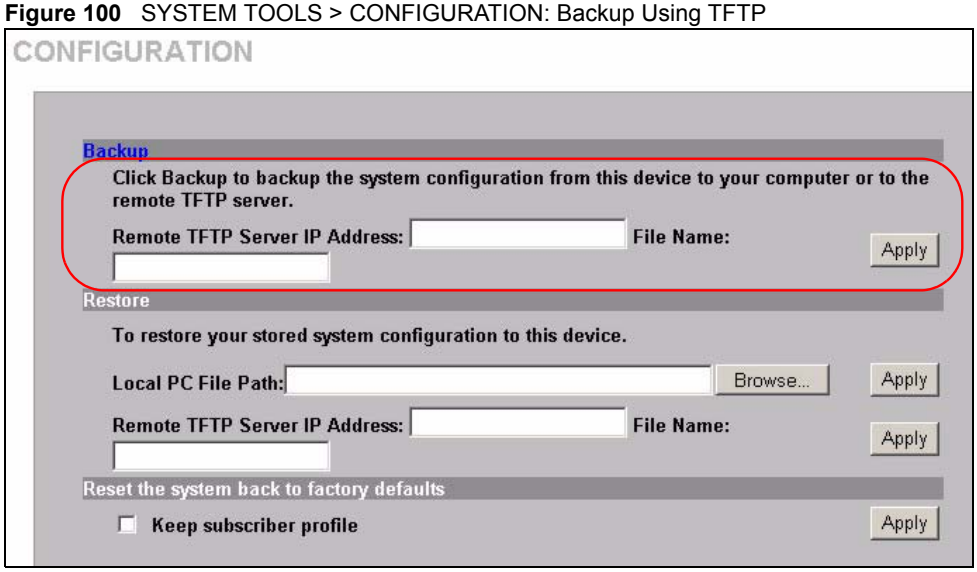
4 Specify the file name and/or location and click **Save** to start the backup process.

27.2.2 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.

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

Figure 100 SYSTEM TOOLS > CONFIGURATION: Backup Using TFTP



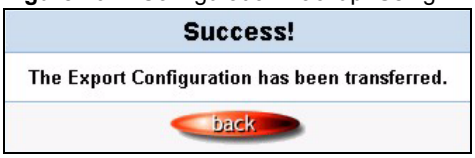
2 Enter the IP address of the TFTP server in dotted decimal notation in the **Remote TFTP Server IP Address** field.

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

Downloaded from www.Manualslib.com manuals search engine

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

Figure 101 Configuration Backup: Using TFTP Successful



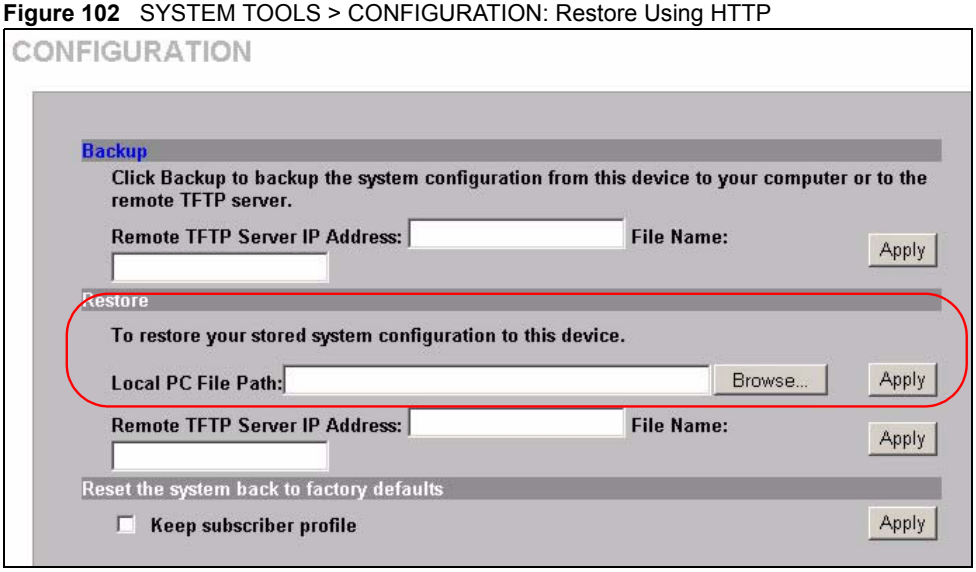
27.2.3 Restore Configuration Using HTTP

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

Note: 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.

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

Figure 102 SYSTEM TOOLS > CONFIGURATION: Restore Using HTTP



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

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

27.2.4 Restore Configuration Using TFTP

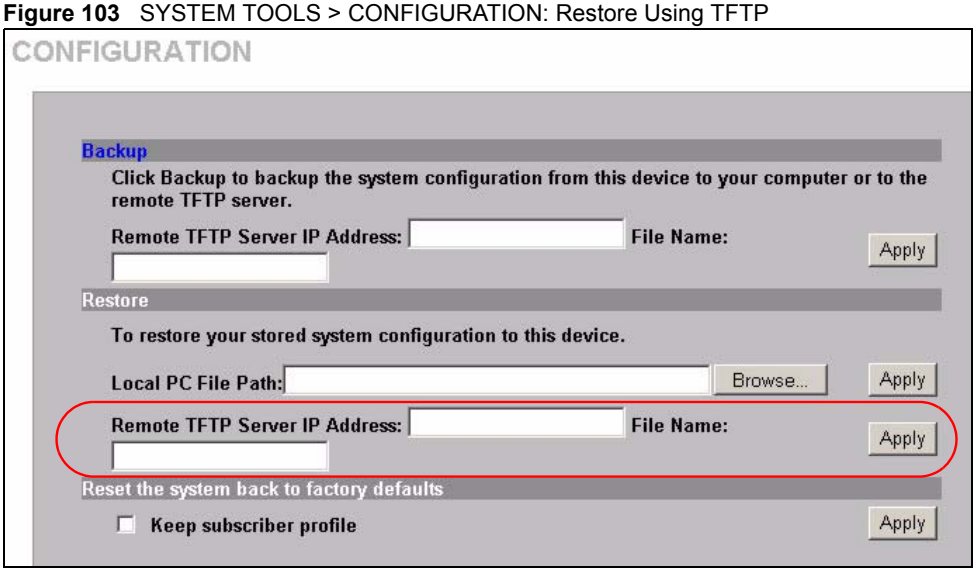
This section shows you how to upload a new or previously saved configuration file from a TFTP server to your ZyXEL Device.

Downloaded from www.Manualslib.com manuals search engine

Note: 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.

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

Figure 103 SYSTEM TOOLS > CONFIGURATION: Restore Using TFTP



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

3 Specify the file name of the configuration file in the **File Name** field.

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

27.3 Firmware Upgrade

There are two ways to upgrade firmware to the ZyXEL Device: 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 ZyXEL Device. You can upload it to the ZyXEL Device using the Web Configurator or using a TFTP server.

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

Note: If you are upgrading to firmware version v1.00(ZB.3)c0 or higher from a lower version, you might upgrade the boot code to v1.03 as well. In this case, you must upgrade the firmware BEFORE you upgrade the boot code.

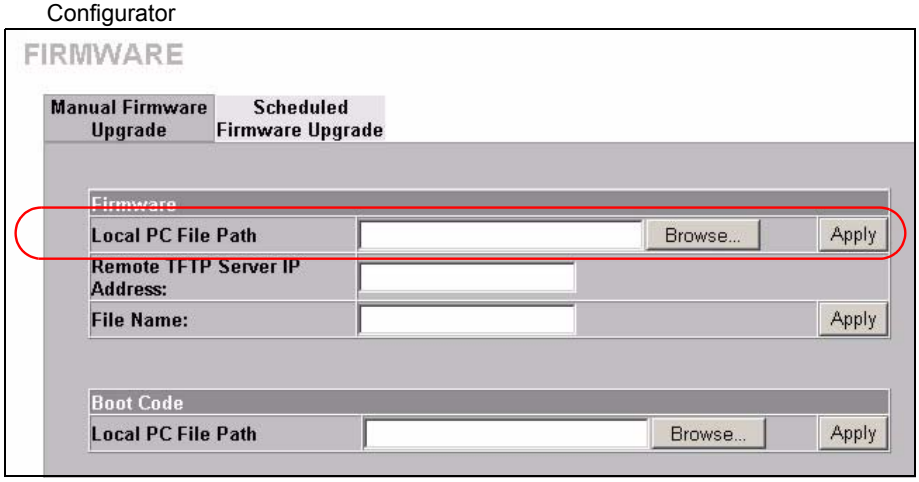
Downloaded from www.Manualslib.com manuals search engine

27.3.1 Manual Firmware Upgrade Using the Web Configurator

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

1 Click **SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade** to display the screen as shown.

Figure 104 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: Using the Web Configurator

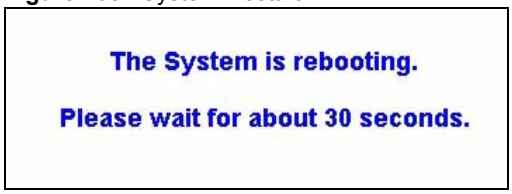


2 Specify the name of the firmware file in the **Local PC File Path** field or click **Browse** to locate the file and click **Apply** to start the file transfer process. The firmware must be a binary file and should have a .bin extension.

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

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

Figure 105 System Restart



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

Note: When the ZyXEL Device restarts, all connections terminate. Subscribers need to log in again.

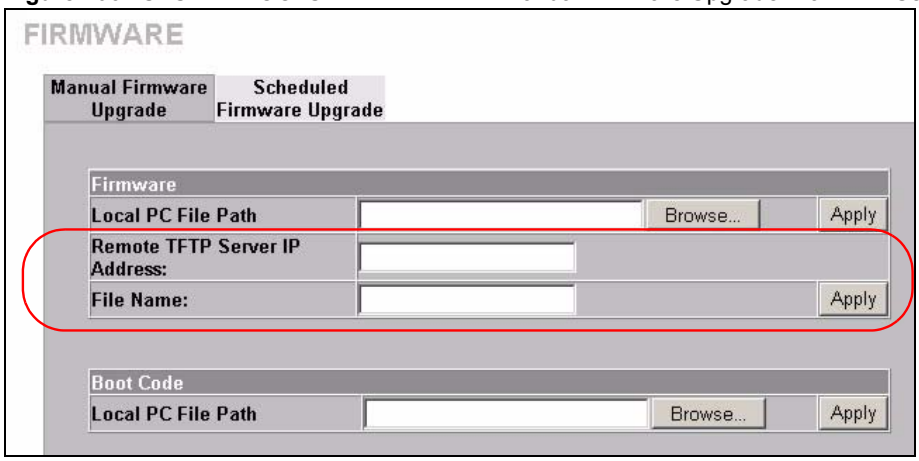
Downloaded from www.Manualslib.com manuals search engine

27.3.2 Manual Firmware Upgrade via TFTP Server

Use the following procedure to use TFTP to upload the firmware from a TFTP server to the ZyXEL Device.

1. Download the latest firmware from www.zyxel.com and store it in a TFTP server. Unzip the file if it is zipped.
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.
3. Access the web configurator. Refer to the section on accessing the web configurator for instructions.
4. Click **SYSTEM TOOLS >, FIRMWARE > Manual Firmware Upgrade** to display the screen as shown.

Figure 106 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: via TFTP Server



5. Specify the IP address of the TFTP server in the **Remote TFTP Server IP Address** field.
6. Specify the name of the firmware file in the **File Name** field.
7. Click **Apply** to start the file transfer process.
8. When the file transfer is completed successfully, the following message displays and the ZyXEL Device restarts automatically to complete the firmware upgrade process.
9. After the ZyXEL Device finishes restarting, access the web configurator again. Check the firmware version number in the **System Status** screen.

27.3.3 Manual Boot Code Upgrade Using the Web Configurator

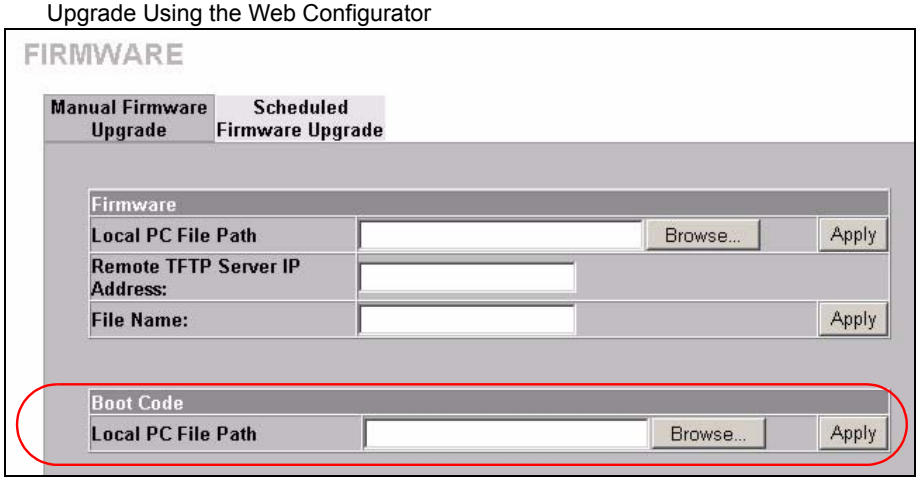
Note: You might upgrade the boot code to v1.03 only if you are upgrading to firmware version v1.00(ZB.3)c0 or higher from a lower version. In this case, you must upgrade the firmware BEFORE you upgrade the boot code.

Downloaded from www.Manualslib.com manuals search engine

Follow the steps below to upload the boot code using the web configurator.

1 Click **SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade** to display the screen as shown.

Figure 107 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: Boot Code Upgrade Using the Web Configurator

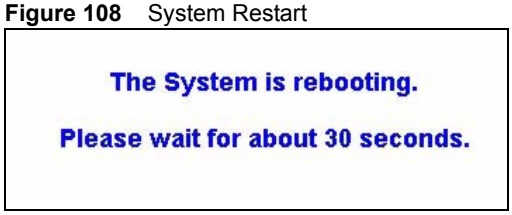


2 Specify the name of the boot code file in the **Local PC File Path** field or click **Browse** to locate the file and click **Apply** to start the file transfer process. The boot code must be a binary file and should have a .rom extension.

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

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

Figure 108 System Restart



4 After the ZyXEL Device finishes restarting, access the web configurator again. Check the Boot ROM version number in the **System** screen.

Note: When the ZyXEL Device restarts, all connections terminate. Subscribers need to log in again.

Downloaded from www.Manualslib.com manuals search engine

27.3.4 Scheduled Firmware Upgrade

Click **SYSTEM TOOLS > FIRMWARE > Scheduled Firmware Upgrade** to display the screen as shown.

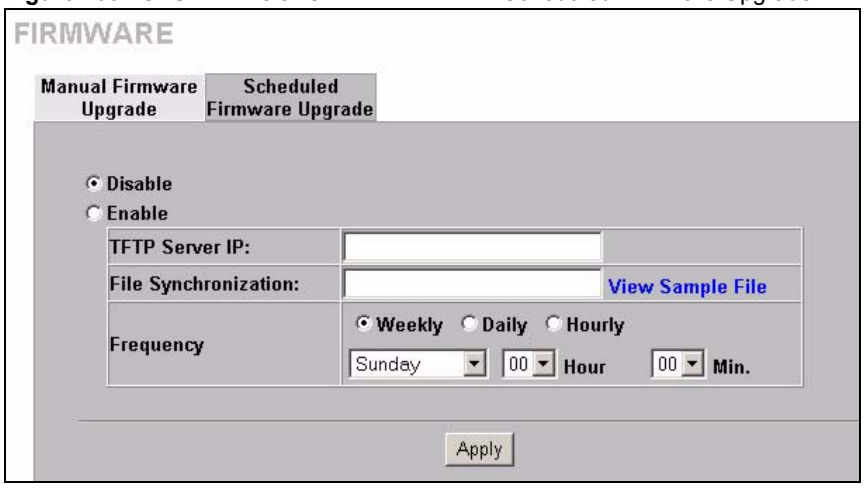
Configure the screen to automatically download the latest firmware from a TFTP server.

Note: 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.

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

Figure 109 SYSTEM TOOLS > FIRMWARE > Scheduled Firmware Upgrade



Note: When the ZyXEL Device restarts, all connections terminate. Subscribers need to log in again.

SYSTEM TOOLS > FIRMWARE > 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 ZyXEL Device 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 see an example synchronization check file.

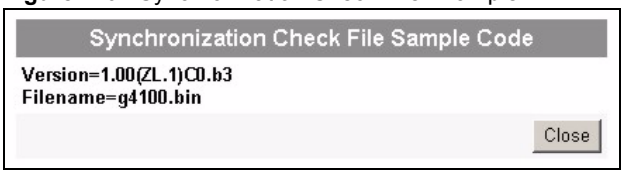
Downloaded from www.Manualslib.com manuals search engine

SYSTEM TOOLS > FIRMWARE > Scheduled Firmware Upgrade (continued)

LABEL	DESCRIPTION
Frequency	Set how often (**Weekly**, **Daily** or **Hourly**) you want to have the ZyXEL Device 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 ZyXEL Device 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 110 Synchronization Check File Example



Downloaded from www.Manualslib.com manuals search engine

CHAPTER 28
SSL (Secure Socket Layer) Security

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

28.1 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 ZyXEL Device and the web browser on a connected computer.

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

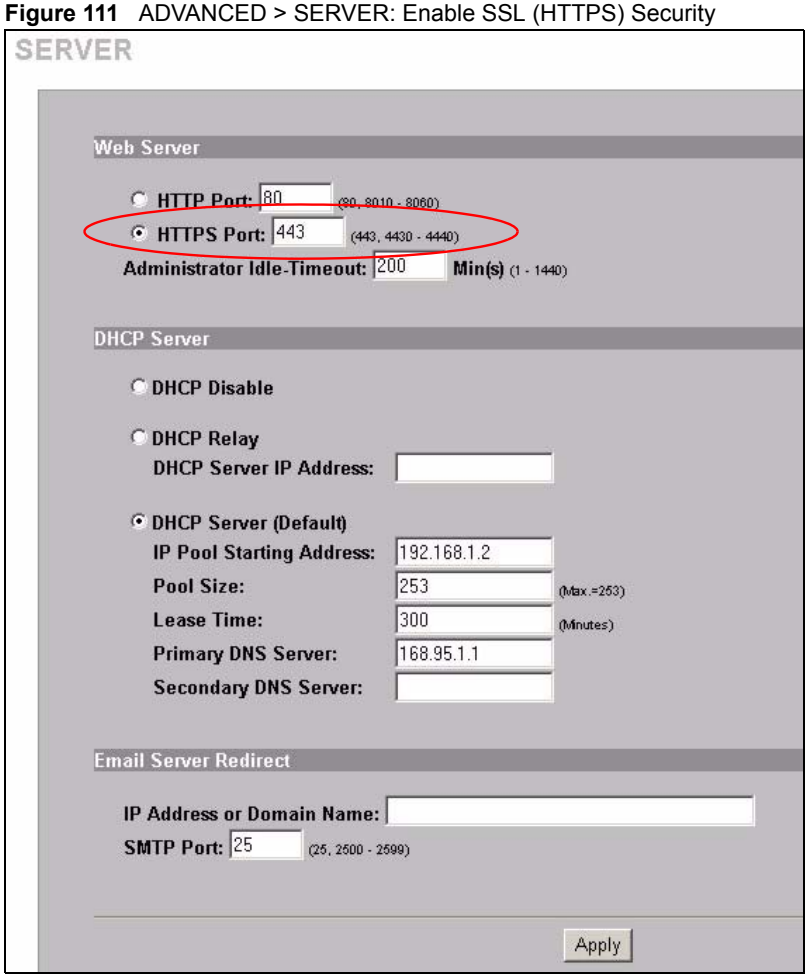
28.2 Activating SSL Security for Management Connections

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

1 Click **ADVANCED** > **SERVER**. Select **HTTPS** under **Web Server**.

Downloaded from www.Manualslib.com manuals search engine

Figure 111 ADVANCED > SERVER: Enable SSL (HTTPS) Security



2 Click **Apply** to save the changes and restart the ZyXEL Device when prompted. See Section 28.3 on page 212 for details on how to install the SSL security certificate in order to access the web configurator through a secure connection.

28.3 Viewing and Installing the SSL Security Certificate

After you enable and activate the SSL security on the ZyXEL Device, 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.

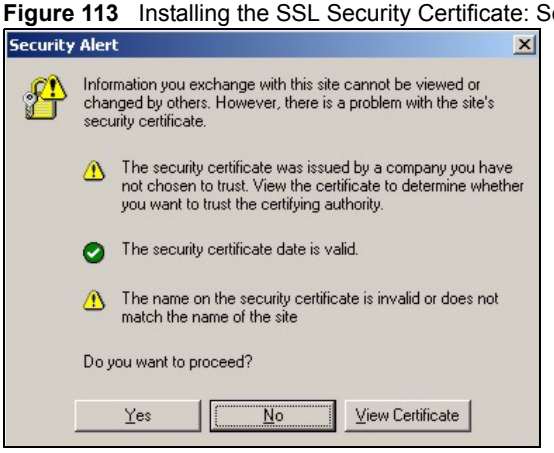
1 Access the ZyXEL Device. A **Security Alert** window displays. Click **OK** to continue and close the window.

Downloaded from www.Manualslib.com manuals search engine

Figure 112 Installing the SSL Security Certificate: First Security Alert

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

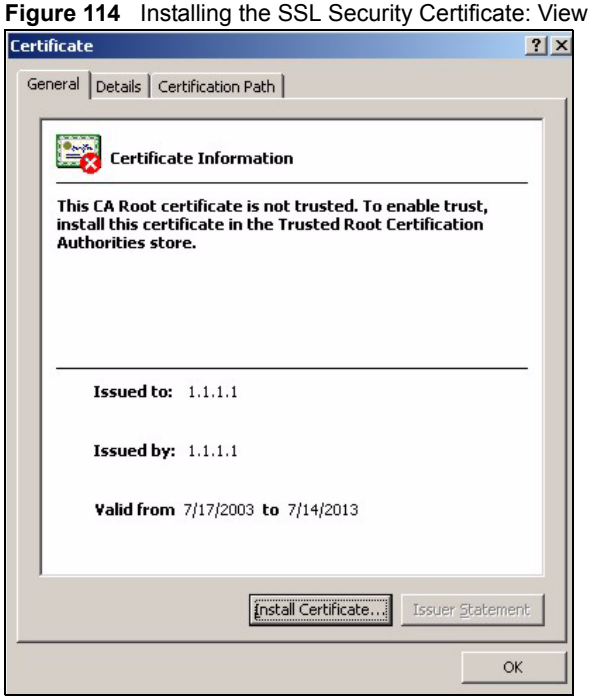
Figure 113 Installing the SSL Security Certificate: Second Security Alert



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

Downloaded from www.Manualslib.com manuals search engine

Figure 114 Installing the SSL Security Certificate: View Certificate



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

Figure 115 Installing the SSL Security Certificate: Certificate Import Wizard

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

Downloaded from www.Manualslib.com manuals search engine

Figure 116 Certificate Import Wizard: Location

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

Figure 117 Certificate Import Wizard: Finish

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

Downloaded from www.Manualslib.com manuals search engine

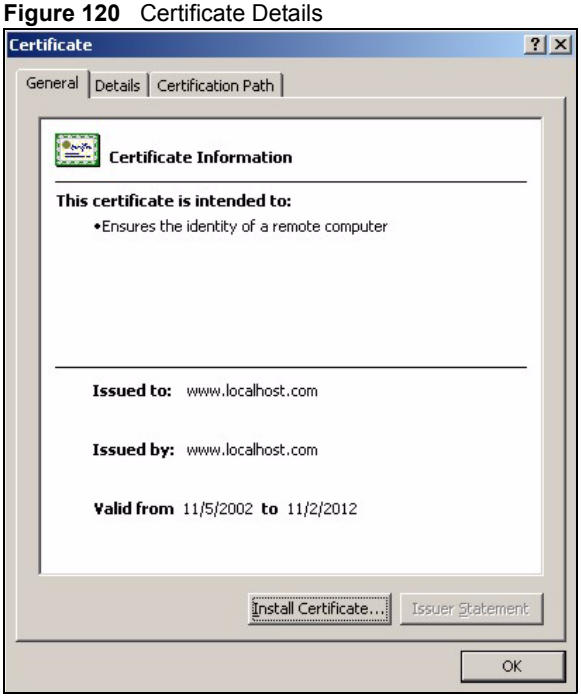
Figure 118 Root Certificate Store

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

Figure 119 Certificate Import Wizard

9 A **Certificate** window displays details.

Figure 120 Certificate Details



Downloaded from www.Manualslib.com manuals search engine

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 121 Security Alert: Trusted

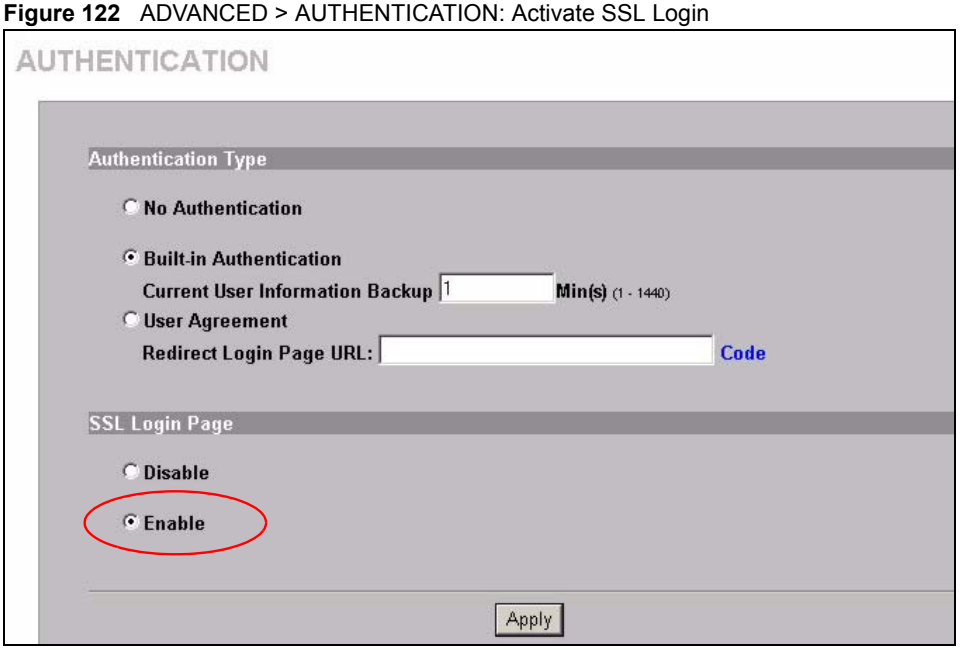
28.4 Activating SSL Security for Subscriber Logins

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

1 Click **ADVANCED > AUTHENTICATION** and select the **Enable** in the **SSL Login Page** field

Downloaded from www.Manualslib.com manuals search engine

Figure 122 ADVANCED > AUTHENTICATION: Activate SSL Login



2 Click **Apply** to save the changes and restart the ZyXEL Device when prompted.

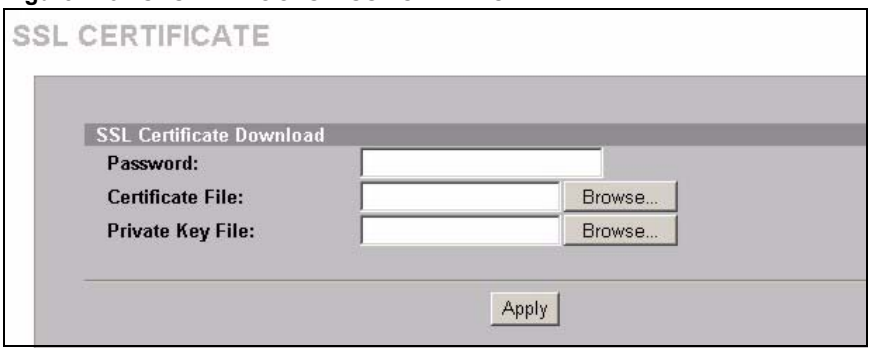
28.5 SSL Certificate Download

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 ZyXEL Device.

Note: You must save the certificate and private key files from the CA on a computer that is connected to the ZyXEL Device.

Figure 123 SYSTEM TOOLS > SSL CERTIFICATE



Downloaded from www.Manualslib.com manuals search engine

The following table describes the labels in this screen.

Table 55 SYSTEM TOOLS > 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 ZyXEL Device.

After you download the certificate files, click Apply to restart the ZyXEL Device.

Note: See the chapter on general system setup for how to set the ZyXEL Device to use the certificate that you download.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 29
Ping Command

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

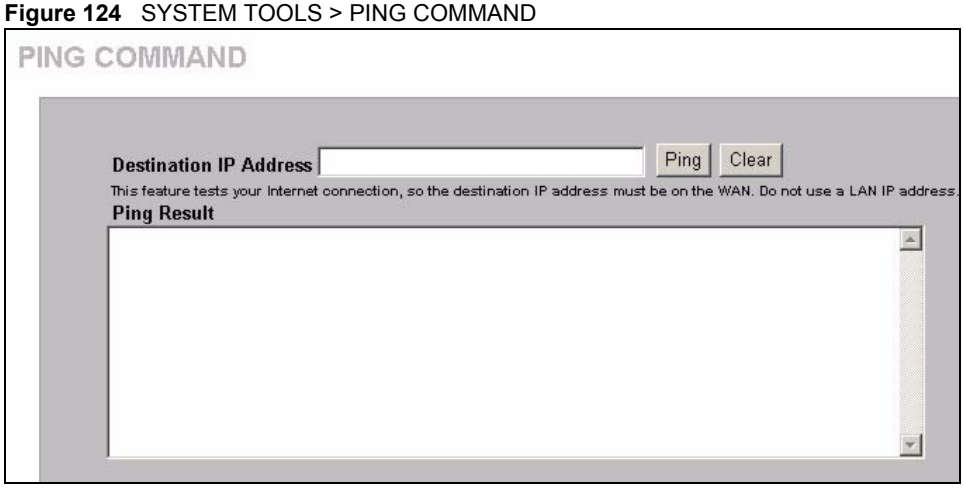
29.1 About Ping Command

Use the ping function to check the ZyXEL Device's network connection.

29.2 Using Ping Command

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

Figure 124 SYSTEM TOOLS > PING COMMAND



The following table describes the labels in this screen.

Table 56 SYSTEM TOOLS > PING COMMANDT

LABEL	DESCRIPTION
Destination IP Address	Type the IP address of a device on the WAN that you want to ping in order to test the Internet connection. **Note:** This feature tests your Internet connection, so the destination IP address must be on the WAN. Do not use a LAN IP address.
Ping	Click this button to have the device ping the IP address.

Downloaded from www.Manualslib.com manuals search engine

Table 56 SYSTEM TOOLS > PING COMMANDT (continued)

LABEL	DESCRIPTION
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.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 30
Restart

This chapter covers how to use the **RESTART** screen.

30.1 Restart

Click **SYSTEM TOOLS > RESTART** to open the following screen. Click Apply to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 125 SYSTEM TOOLS > RESTART

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 31
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.

31.1 Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

31.1.1 The Power LED

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

Table 57 Troubleshooting Power LED

STEPS	CORRECTIVE ACTION
1	Check the connection from the ZyXEL Device 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 ZyXEL Device is receiving sufficient power.
3	If these steps fail to correct the problem, contact your local distributor for assistance.

31.1.2 The LAN Port LEDs

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

Table 58 Troubleshooting LAN LEDs

STEPS	CORRECTIVE ACTION
1	Make sure the ZyXEL Device is turned on.
2	Verify that the attached device(s) is turned on and properly connected to the ZyXEL Device.
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).

Downloaded from www.Manualslib.com manuals search engine

31.1.3 The WAN Port LED

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

Table 59 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 ZyXEL Device.
3	Verify that the Ethernet cable length does not exceed 100 meters.

31.2 Web Configurator

I cannot access the web configurator.

Table 60 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 ZyXEL Device 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 ZyXEL Device. All of your custom configuration will be lost.
4	Ping the ZyXEL Device from your computer on the WAN or LAN. If you cannot ping the ZyXEL Device, check the IP addresses of the ZyXEL Device 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.

Downloaded from www.Manualslib.com manuals search engine

The web configurator does not display properly.

Table 61 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.)

31.3 Internet Access

A subscriber cannot connect to the Internet through the ZyXEL Device.

Table 62 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 ZyXEL Device. The user name and password are case sensitive.
3	Verify that the IP addresses and the subnet masks of the ZyXEL Device 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 ZyXEL Device and wireless client(s) are using the same ESSID, channel and WEP key (if WEP encryption is activated).

31.4 Statement Printer

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

I cannot print subscriber statements using a statement printer.

Table 63 Troubleshooting a 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 ZyXEL Device via Ethernet.
3	Make sure there is enough printing paper in the statement printer.

Downloaded from www.Manualslib.com manuals search engine

Table 63 Troubleshooting a Statement Printer (continued)

STEPS	CORRECTIVE ACTION
4	Make sure you set the ZyXEL Device to require authentication before allowing Internet access, see the Wizard Setup screens or the **Authentication** chapter.
5	Make sure the IP address of the statement printer is configured in the **Account Generator** screen. See Chapter 22 on page 169. Also make sure that the ZyXEL Device and the statement printer(s) are using the same port number. If you are using encryption with the statement printer(s), make sure the secret key is correctly configured in the **Account Generator** screen and the statement printer(s). See Chapter 22 on page 169 and the statement printer user's guide.

Downloaded from www.Manualslib.com manuals search engine

APPENDIX A
Product Specifications

Product Feature Specifications

Firmware Specifications

Table 64 Firmware Specifications

IP Plug and Play (iPnP technology)	Zero Configuration IP Plug and Play Internet Access
Networking Functions	NAT Various WAN connections (Static IP/DHCP Client/PPPoE/PPTP) DHCP Server HTTP Proxy Server NTP (Network Time Protocol) support
User Authentication and Accounting	Supports up to 100 concurrent users Web-based Authentication Idle-timeout Control
Security and Firewall	Layer 2 Isolation SSL Login Page and Administration VPN (IPSec/PPTP/L2TP) Pass through Custom SSL Certificate Administration Access Control
Management	Web-based management tool TFTP/HTTP firmware upgrade Scheduled firmware upgrade Backup/Restore Configuration file SNMP MIBII supported LAN devices Management LAN devices Status Monitor Session List Syslog Default printer (SP-200E) support
Marketing Cooperation	Pass through IP/MAC/URL Custom Login Page Login Page Redirect Advertisement URL link Walled garden Portal page redirection

Downloaded from www.Manualslib.com manuals search engine

Wireless Specifications

Table 65 Wireless Specifications

Network Standard	IEEE 802.11b IEEE 802.11g
Frequency Band	2.400~2.472GHz
Data Rate	IEEE 802.11g(auto-fallback) -OFDM: 54, 48, 36, 24, 18, 12, 9 and 6Mbps IEEE 802.11b(auto-fallback) -CCK: 11, 5.5Mbps -DQPSK: 2 Mbps -DBPSK: 1 Mbps
Media Access Control	CSMA/CA with ACK
Channel	IEEE 802.11g Ch. 1~11 N. America Ch. 1~13 Japan Ch. 1~13 Europe ETSI IEEE 802.11b Ch. 1~11 N. America Ch. 1~13 Japan Ch. 1~13 Europe ETSI
Transmission	IEEE 802.11b (DSSS), IEEE 802.11g (OFDM)
Modulation	IEEE 802.11b (DSSS), CCK @ 11, 5.5Mbps DQPSK @ 2 Mbps DBPSK @ 1 Mbps IEEE 802.11g (OFDM) BPSK @ 6, 9 Mbps QPSK@ 12, 18 Mbps 16-QAM@ 24, 36 Mbps 64-QAM@ 48, 54 Mbps
Network Architecture	Infrastructure Mode
Output Power	IEEE 802.11g 54 Mbps 14+/-2dBm IEEE 802.11b 11 Mbps 16+/-2dBm

Hardware Specifications

Table 66 Hardware Specifications

Network Specification	IEE802.3 10BaseT Ethernet IEE802.3u 100BaseTX Fast Ethernet IEE802.11g Wireless LAN ANSI/IEEE 802.3 NWay auto-negotiation
Compatibility	Can communicate with Wi-Fi certificated wireless adapters
Connectors	4 LAN Ports and One WAN Port 10/100BaseTX with auto MDI/MDI-X RS-232 port (For debugging and testing purpose only)
Wireless Operation Range	Open Space: 100~300m Indoors: 35~100m
Wireless Data Rate	Up to 54 Mbps for IEEE 802.11g with auto fallback to IEEE 802.11b

Downloaded from www.Manualslib.com manuals search engine

Table 66 Hardware Specifications (continued)

Encryption	WEP 64/128, WPA
External Antenna	Two 2dBi (Max) Dual detachable diversity antennas with reverse SMA connectors
Power Requirement	External Power Adapter Input: 100-240 VAC, 50/60 Hz, 0.35 A Output: 5V, 2A POE
Dimensions	Size: 212.5 (L) x 138.5(W) x 52.0(H) mm Net Weight: 508g
Environment Conditions	Operating Temperature:0 to 50'C Storage Temperature: -30 to 60'C Humidity: Max. 90% non-condensing
Mounting	Desktop Wall mounted
LED Indicators	One **PWR** LED One **WAN** Link/Activity LED Four **LAN** Link/Activity LEDs One **SYS** LED One blue (**ZyAIR)** Wireless Link/Activity LED

Certifications

Table 67 Certifications

Certifications	FCC part 15 Class B CE / R&TTE CSA Internal with ZyXEL file number C-Tick

Power over Ethernet (POE)

- The ZyXEL Device is compatible with IEEE 802.3af so it can receive power through an Ethernet cable. Use standard 8-wire CAT 5 10/100 BaseT Ethernet cable to connect an IEEE 802.3af compatible power injector to the **WAN** port.
- The ZyXEL Device receives DC power through the unused twisted-wires (pairs 4/5 and 7/8) of the Ethernet cable.

RJ-45 Ethernet Ports

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

Downloaded from www.Manualslib.com manuals search engine

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

Table 68 Network 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

WAN Port

The following figure and table describe the Ethernet cable pin assignments for the WAN port.

Figure 126 WAN Port Cable Pin Assignments

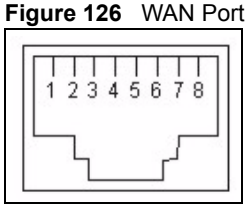


Table 69 WAN Port Cable Pin Assignments

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 ZyXEL Device and the switch or router conforms to the following pin assignments.

Table 70 WAN Port Cable Pin Assignments

ETHERNET DEVICE (SWITCH/HUB/ROUTER ETC.)		ZYXEL DEVICE	
1	RD+	1	TD+
2	RD-	2	TD-

Downloaded from www.Manualslib.com manuals search engine

Table 70 WAN Port Cable Pin Assignments (continued)

ETHERNET DEVICE (SWITCH/HUB/ROUTER ETC.)		ZYXEL DEVICE	
3	TD+	3	RD+
6	TD-	6	RD-

LAN Ports

The following figure and table describe the Ethernet cable pin assignments for the LAN port.

Figure 127 LAN Port Cable Pin Assignments

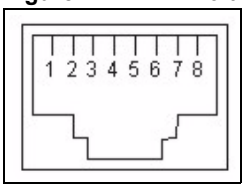


Table 71 LAN Port Cable Pin Assignments

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.

Table 72 LAN Port Cable Pin Assignments

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

Downloaded from www.Manualslib.com manuals search engine

CONSOLE Port

The ZyXEL Device does not currently use this port.

Antenna Connector Type

The ZyXEL Device is equipped with reverse polarity SMA jacks.

Antenna Specifications

2.4GHz wireless antennas with reverse polarity SMA plugs are included.

Downloaded from www.Manualslib.com manuals search engine

Appendix B
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.

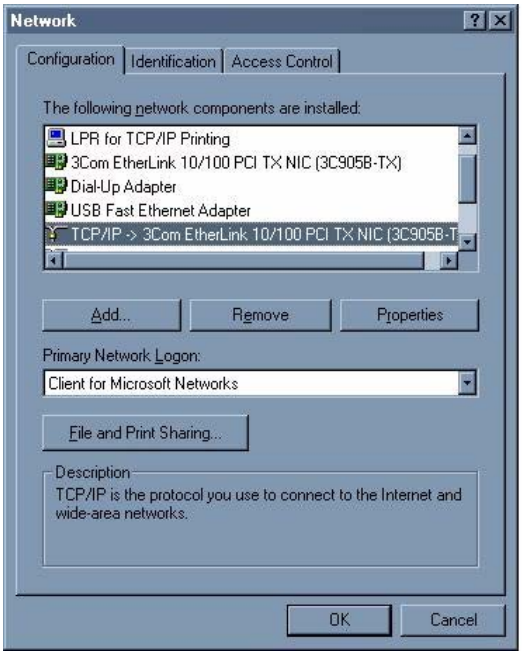
If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Downloaded from www.Manualslib.com manuals search engine

Figure 128 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.

Downloaded from www.Manualslib.com manuals search engine

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

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

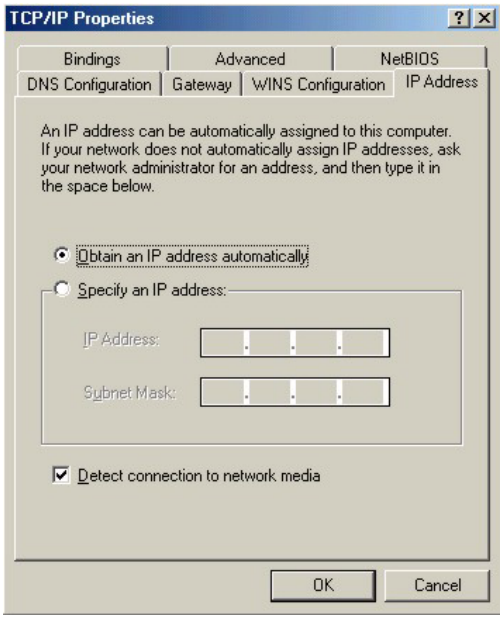
Configuring

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

2 Click the **IP Address** tab.

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

Figure 129 Windows 95/98/Me: TCP/IP Properties: IP Address

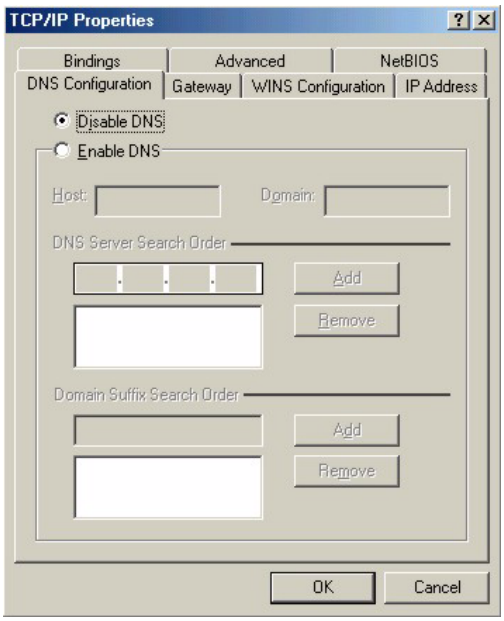


3 Click the **DNS** Configuration tab.

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

Downloaded from www.Manualslib.com manuals search engine

Figure 130 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

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

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

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Downloaded from www.Manualslib.com manuals search engine

Figure 131 Windows XP: Start Menu

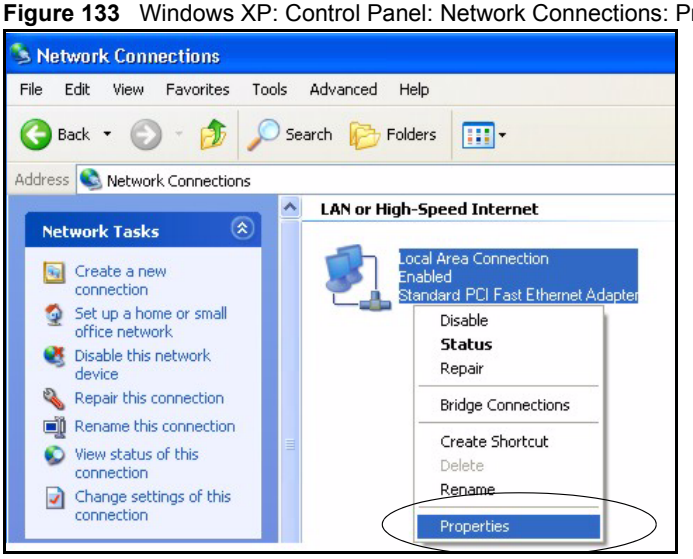
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 132 Windows XP: Control Panel

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

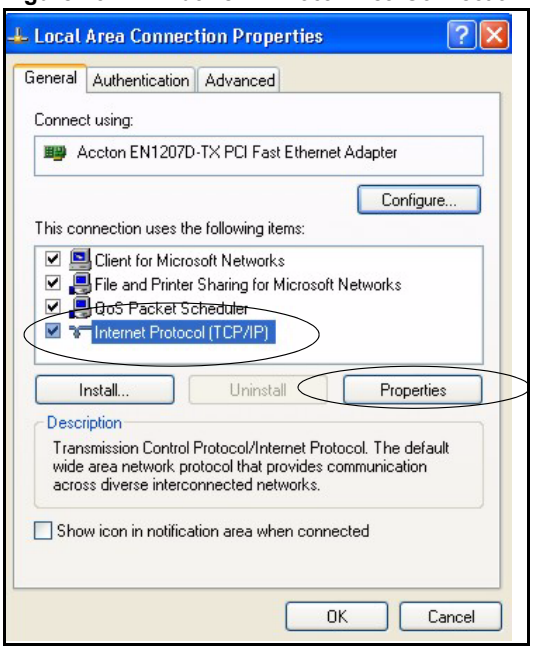
Downloaded from www.Manualslib.com manuals search engine

Figure 133 Windows XP: Control Panel: Network Connections: Properties



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

Figure 134 Windows XP: Local Area Connection Properties



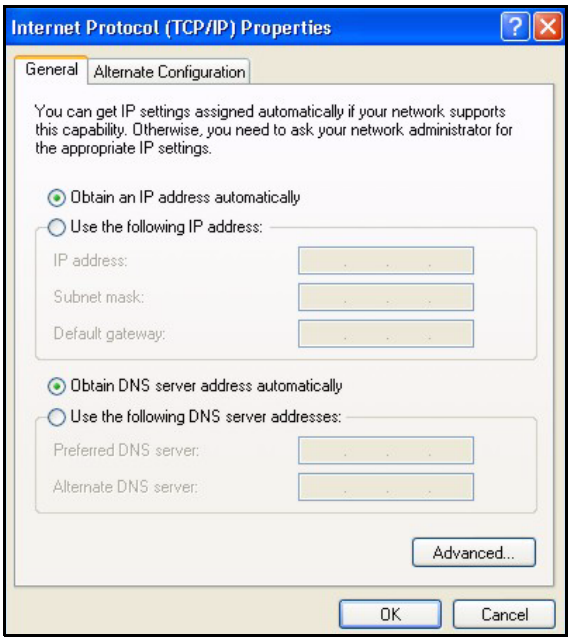
5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

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

Downloaded from www.Manualslib.com manuals search engine

- Click **Advanced**.

Figure 135 Windows XP: Internet Protocol (TCP/IP) Properties



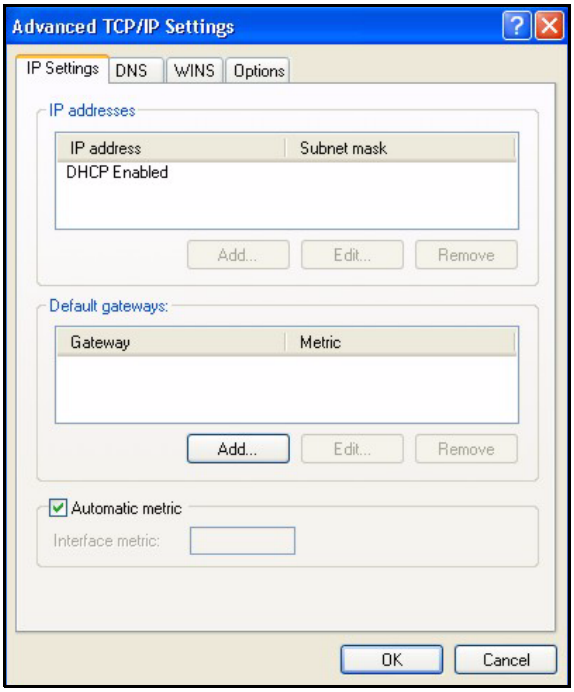
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Downloaded from www.Manualslib.com manuals search engine

Figure 136 Windows XP: Advanced TCP/IP Properties



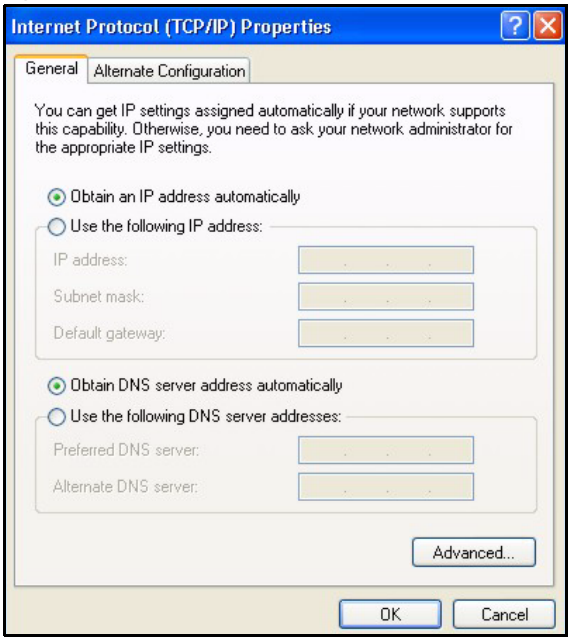
7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- 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.

Downloaded from www.Manualslib.com manuals search engine

Figure 137 Windows XP: Internet Protocol (TCP/IP) Properties



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

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

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

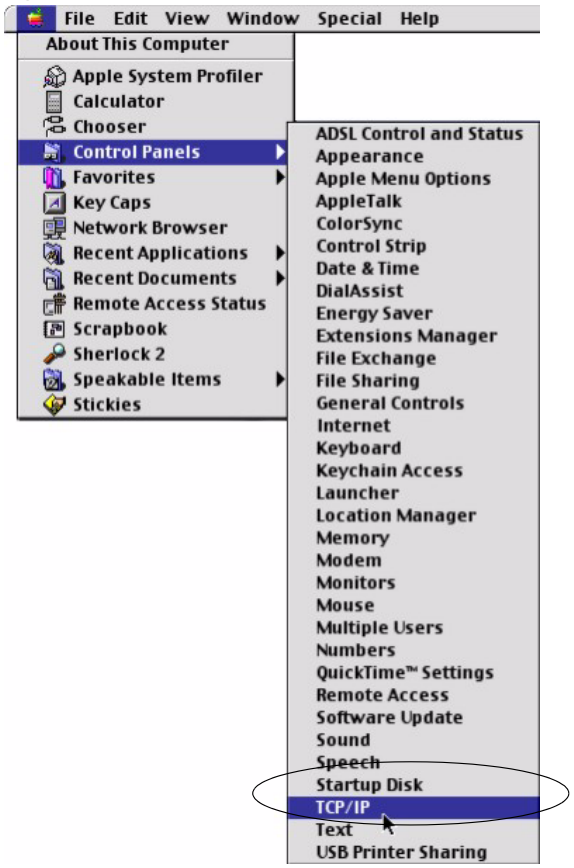
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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

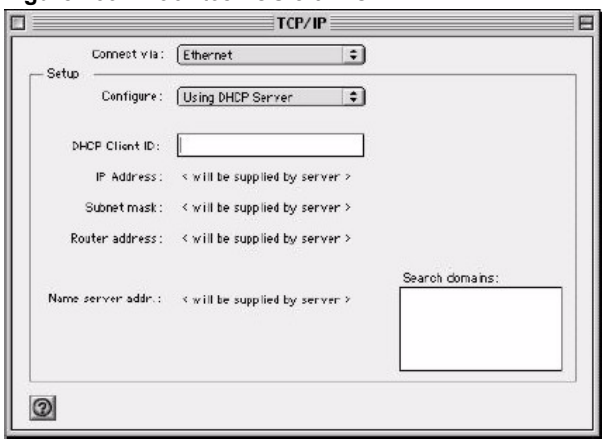
Downloaded from www.Manualslib.com manuals search engine

Figure 138 Macintosh OS 8/9: Apple Menu



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

Figure 139 Macintosh OS 8/9: TCP/IP



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

Downloaded from www.Manualslib.com manuals search engine

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 Prestige 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 Prestige and restart your computer (if prompted).

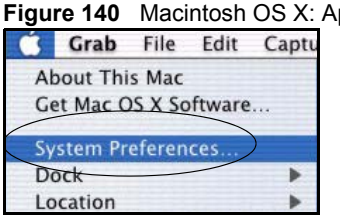
Verifying Settings

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

Macintosh OS X

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

Figure 140 Macintosh OS X: Apple Menu

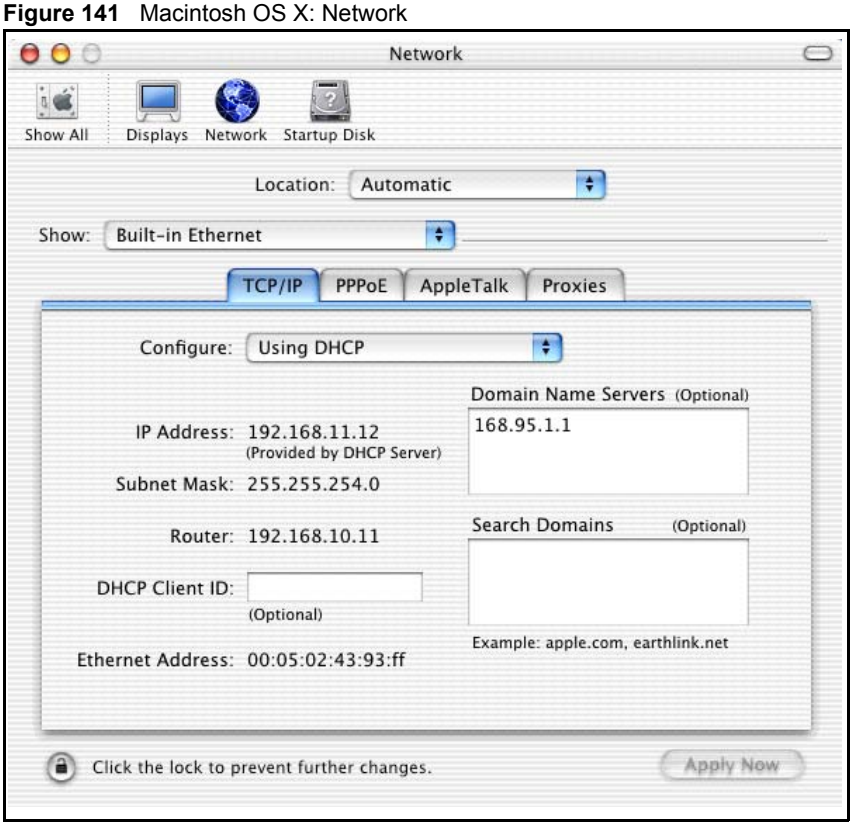


2 Click **Network** in the icon bar.
   - Select **Automatic** from the **Location** list.
   - Select **Built-in Ethernet** from the **Show** list.
   - Click the **TCP/IP** tab.

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

Downloaded from www.Manualslib.com manuals search engine

Figure 141 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

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

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

Downloaded from www.Manualslib.com manuals search engine

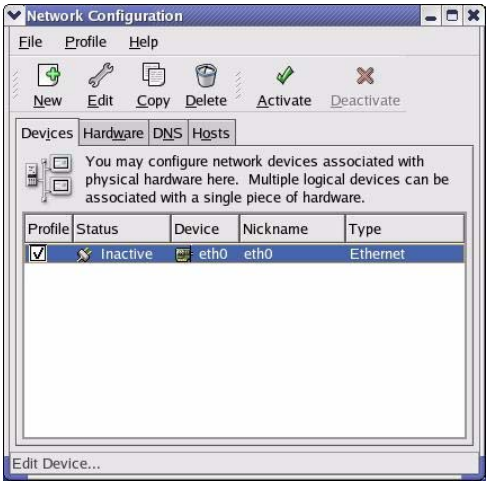
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 142 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 143 Red Hat 9.0: KDE: Ethernet Device: General

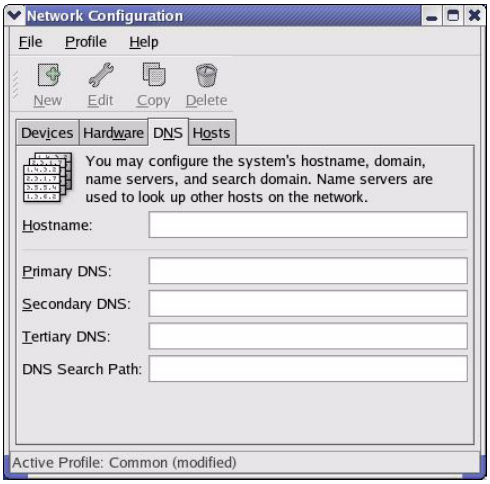
Downloaded from www.Manualslib.com manuals search engine

- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

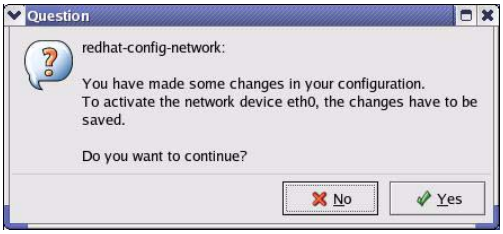
Figure 144 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

Figure 145 Red Hat 9.0: KDE: Network Configuration: Activate



7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

Downloaded from www.Manualslib.com manuals search engine

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 146 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 147 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 148 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Downloaded from www.Manualslib.com manuals search engine

Figure 149 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                 [OK]
Shutting down loopback interface:             [OK]
Setting network parameters:                   [OK]
Bringing up loopback interface:               [OK]
Bringing up interface eth0:                   [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 150 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```


Downloaded from www.Manualslib.com manuals search engine

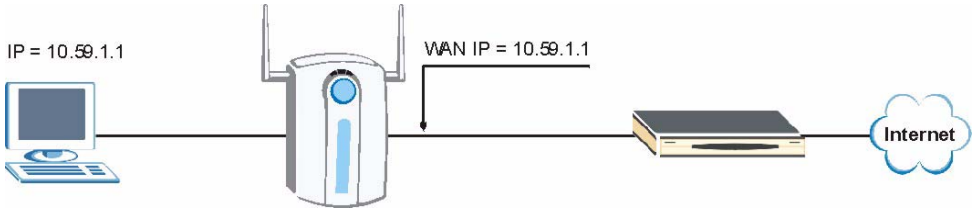
Appendix C
IP Address Assignment Conflicts

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 ZyXEL Device is using the same LAN and WAN IP addresses

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

Figure 151 IP Address Conflicts: Case A



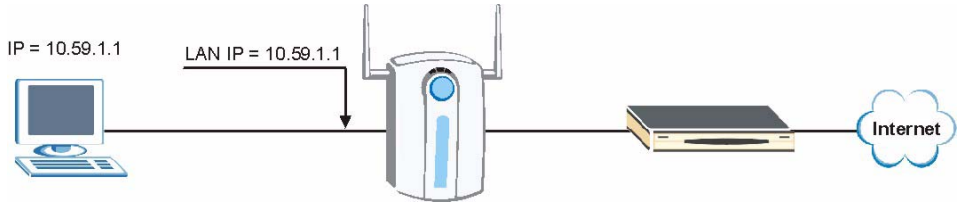
You must set the ZyXEL Device to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyXEL Device. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyXEL Device use a public WAN IP address.

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

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

Downloaded from www.Manualslib.com manuals search engine

Figure 152 IP Address Conflicts: Case B

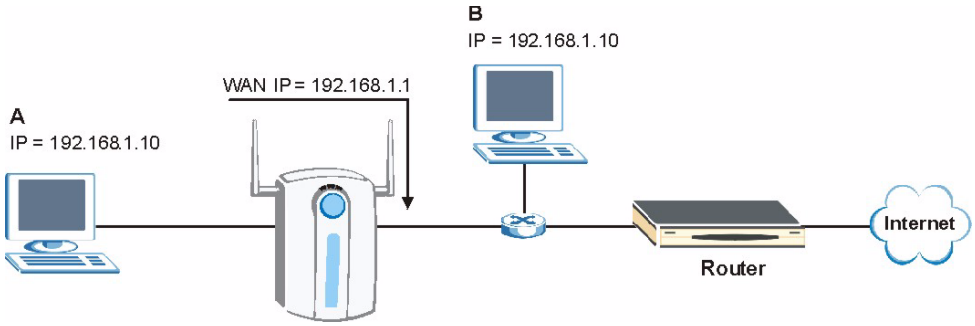


To solve this problem, make sure the ZyXEL Device LAN IP address is not in the DHCP IP address pool.

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 ZyXEL Device.

Figure 153 IP Address Conflicts: Case C



You must set the ZyXEL Device to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyXEL Device. 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 ZyXEL Device use a public WAN IP address.

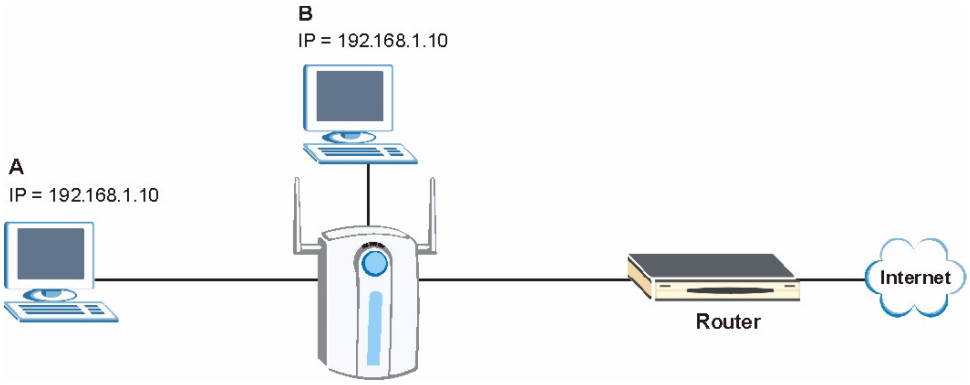
Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the ZyXEL Device 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 ZyXEL Device DHCP server assigns to another subscriber acting as a DHCP client.

Downloaded from www.Manualslib.com manuals search engine

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

Figure 154 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.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Appendix D
Indoor Installation Recommendations

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

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

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

Radiation Pattern

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

Antenna Gain

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

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

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

Types of Antennas For WLAN

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

Downloaded from www.Manualslib.com manuals search engine

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

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

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

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

Downloaded from www.Manualslib.com manuals search engine

Appendix E
Wireless LANs

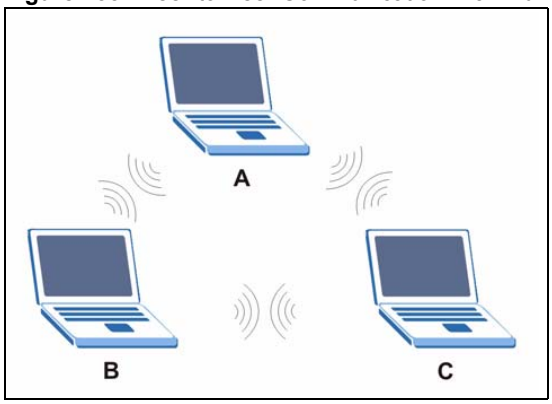
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 155 Peer-to-Peer Communication in an Ad-hoc Network



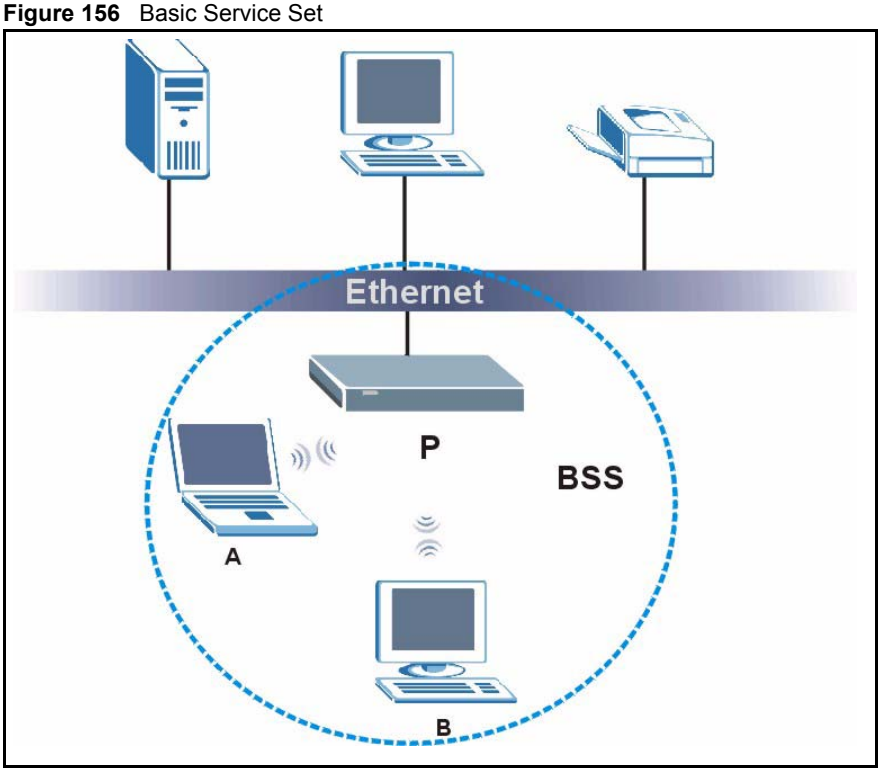
BSS

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

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Downloaded from www.Manualslib.com manuals search engine

Figure 156 Basic Service Set



ESS

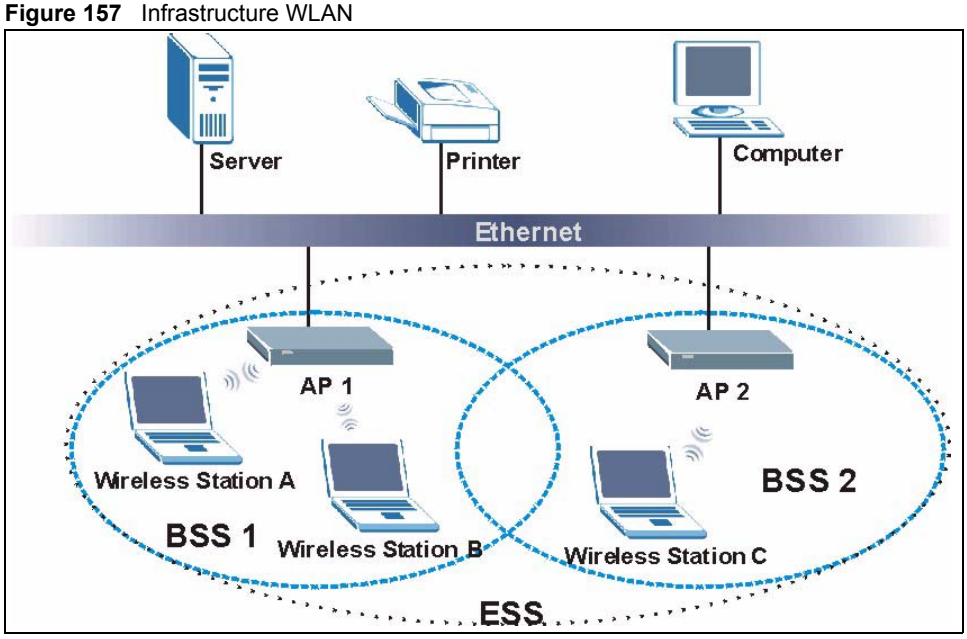
An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Downloaded from www.Manualslib.com manuals search engine

Figure 157 Infrastructure WLAN



Channel

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

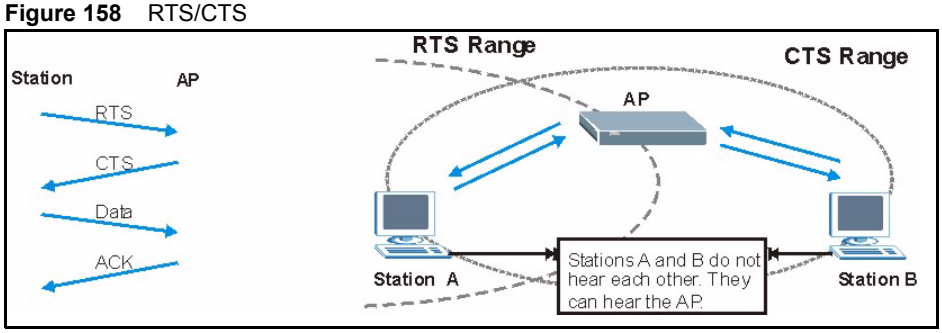
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel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

RTS/CTS

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

Downloaded from www.Manualslib.com manuals search engine

Figure 158 RTS/CTS



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

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

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

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

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

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

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

Fragmentation Threshold

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

Downloaded from www.Manualslib.com manuals search engine

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

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

Preamble Type

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

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

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

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

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

Table 73 IEEE 802.11g

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

Downloaded from www.Manualslib.com manuals search engine

IEEE 802.1x

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

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS

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

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

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

Types of RADIUS Messages

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

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

Downloaded from www.Manualslib.com manuals search engine

- Access-Challenge

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

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

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

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

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

Types of Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

Downloaded from www.Manualslib.com manuals search engine

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

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

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

Note: EAP-MD5 cannot be used with dynamic WEP key exchange

Downloaded from www.Manualslib.com manuals search engine

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 74 Comparison of EAP Authentication Types

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

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 75 Wireless Security Relational Matrix

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

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

APPENDIX F
IP Addresses and Subnetting

This appendix introduces IP addresses, IP address classes and subnet masks. You use subnet masks to subdivide a network into smaller logical networks.

Introduction to IP Addresses

An IP address has two parts: the network number and the host ID. Routers use the network number to send packets to the correct network, while the host ID identifies a single device on the network.

An IP address is made up of four octets, written in dotted decimal notation, for example, 192.168.1.1. (An octet is an 8-digit binary number. Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.)

There are several classes of IP addresses. The first network number (192 in the above example) defines the class of IP address. These are defined as follows:

- Class A: 0 to 127
- Class B: 128 to 191
- Class C: 192 to 223
- Class D: 224 to 239
- Class E: 240 to 255

IP Address Classes and Hosts

The class of an IP address determines the number of hosts you can have on your network.

- In a class A address the first octet is the network number, and the remaining three octets are the host ID.
- In a class B address the first two octets make up the network number, and the two remaining octets make up the host ID.
- In a class C address the first three octets make up the network number, and the last octet is the host ID.

Downloaded from www.Manualslib.com manuals search engine

The following table shows the network number and host ID arrangement for classes A, B and C.

Table 76 Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	**Network number**	Host ID	Host ID	Host ID
Class B	**Network number**	**Network number**	Host ID	Host ID
Class C	**Network number**	**Network number**	**Network number**	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have $2^8 – 2$, or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have $2^{16} – 2$, or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have $2^{24} – 2$ hosts, or approximately 16 million hosts.

IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an address.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

Table 77 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
Class E (reserved)	**1111**0000 to **1111**1111	240 to 255

Downloaded from www.Manualslib.com manuals search engine

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. 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 like IP addresses. The "natural" masks for class A, B and C IP addresses are as follows.

Table 78 "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 leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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

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

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

Table 79 Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224

Downloaded from www.Manualslib.com manuals search engine

Table 79 Alternative Subnet Mask Notation (continued)

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 80 Two Subnets Example

IP/SUBNET MASK	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").

To make two networks, divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

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

Table 81 Subnet 1

IP/SUBNET MASK	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

Downloaded from www.Manualslib.com manuals search engine

Table 81 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 82 Subnet 2

IP/SUBNET MASK	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	

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 (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 zeroes is the subnet itself, all ones is the broadcast address on the subnet).

Table 83 Subnet 1

IP/SUBNET MASK	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

Downloaded from www.Manualslib.com manuals search engine

Table 83 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 84 Subnet 2

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

Table 85 Subnet 3

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

Table 86 Subnet 4

IP/SUBNET MASK	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 eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

Downloaded from www.Manualslib.com manuals search engine

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

Table 87 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

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

Table 88 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 76 on page 268) available for subnetting.

Downloaded from www.Manualslib.com manuals search engine

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

Table 89 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Downloaded from www.Manualslib.com manuals search engine

Index

Numerics

2.4 GHz 175

A

access control 31
account activated 158
account created 158
account deletion 81
account generator 33, 169
account information 124
account log 195
account manager account 42
account printout 112
account printout preview 115
account usage time 78
accounting 31, 79
accounts
  creating 83
accumulation 73, 77, 114
accumulation accounting 75
Address Resolution Protocol (ARP) 50
administrator account 41
administrator idle-timeout 65
advanced subscriber login screen 105
advertisement links 140
advertising links 31
alternative subnet mask notation 269
antenna
  directional 256
  omni-directional 256
antenna gain 255
antennas 32
Any IP 29
  note 50
AP (Access Point) 259
applications 33
article 106
article background color 106
article text color 106
authentication 67
authentication method 181
authorization code 121
Authorize.net 90
  email additional information 90
  merchant ID 90
  merchant name 91
  merchant transaction key 90
  payment gateway 90
auto-negotiation 33

B

background color 103
bandwidth 165
  bandwidth management 166
  maximum downstream 166
  maximum upstream 166
beacon interval 181
billing 75
billing log 158
billing method 114
billing profile 114
Bluetooth 175
bootrom version 193
BSS 173, 257
built-in authentication 68
button presses 82

C

CA 264
cancel button 103
CCK. See Complementary Code Keying.
certificate authority 264
certifications 4
  notices 5
  viewing 5
changing system password 42
channel 175, 194, 259
  interference 259
charge 78
charge by levels 79, 82
choose 28

Downloaded from www.Manualslib.com manuals search engine

Clear to Send 177
code 104, 171
comments 106
Complementary Code Keying 175
conditions 82
configuration and firmware files
  filename convention 201
configuration file
  backup 201, 203
  restore 204
connect on demand 62, 63
connection ID/name 63
contact information 8
copyright 3, 103
coverage 175
credit card 89, 118
credit card code 121
credit card fail 125
credit card icons 91
credit card number 121
credit card service 77
CTS (Clear to Send) 260
currency 77
current user information backup 68
current users 196
customer ID 121
customer support 8
customization 101

D

data encryption 176
data rates 175
daylight saving time 54
DBPSK. See Differential Binary Phase Shift Keyed.
decimal places 77
default gateway 41
default IP gateway 193
default LAN IP address 57
device IP address 148
device name 148
device server port 148
DHCP 30, 57, 193
  client table 197
DHCP client 57, 62
DHCP pool size 66
DHCP server 65
DHCP server IP address 65
Differential Binary Phase Shift Keyed 175
Differential Quadrature Phase Shift Keying 175
disclaimer 3
discount price plan 79, 81
DNS 41, 193
DNS proxy 31
DNS server 62, 66
Domain Name 49
domain name 40, 53, 193
Domain Name System 59
DQPSK. See Differential Quadrature Phase Shift Keying.
Dynamic DNS 143
Dynamic Host Configuration Protocol 57
dynamic WEP key exchange 264
DYNDNS wildcard 143

E

EAP authentication 263
email button 124
e-mail forwarding 31
e-mail redirection 194
email server 155
e-mail server redirect 66
enable credit card service 77
encryption 41, 170, 194
ending 114
enter 28
enter button 103
ESS 258
ESS. See Extended Service Set.
ESSID 41, 114, 174, 193
ethernet cable length limit 232
exclusive printer 33, 85, 169
expiration 81
expiration time 114, 124
Extended Service Set 174, 258
Extended Service Set IDentification 180

F

factory ethernet defaults 57
factory-defaults 44
FCC interference statement 4
features 29

Downloaded from www.Manualslib.com manuals search engine

feedback 27
filename conventions 201
filtering 131
firmware 32
firmware upgrade
  scheduled 209
firmware version 40, 193
footnote 103
fragmentation threshold 177, 181, 260
framed subscriber login screen 108

G

gateway IP address 62
Generic Interface Specification 74
glossary and web site 27

H

help 27
hidden node 259
host name 53, 193

I

IANA 58
IBSS 257
idle time out 73, 77
IEEE 802.11b 32
  data Rates 175
  modulation 175
IEEE 802.11g 32, 175, 261
  data rates 175
  modulation 175
IEEE 802.1Q tagged VLAN 30
Independent Basic Service Set 173, 257
information windows 110
inside server 150
Internet Assigned Numbers Authority. See IANA.
IP address 58
  LAN 62, 193
  WAN 62, 193
IP address assignment 57
IP addresses
  private 58
IP Plug and Play 54
IP pool starting address 65
iPass 74
IPASS GIS 74
iPnP 49, 54
  how it works 50

K

keep alive 62, 63
keypad 93

L

LAN
  IP address 41, 62, 193
  MAC address 41, 193
  subnet mask 41, 62
LAN device 147
  accessing 199
  detecting time 148
  management 147, 149
  port mapping 147
LAN devices 199
LAN devices alarm 158
LAN devices information 158
LAN subnet mask 193
layer 2 isolation security 54
lease time 66
level 82
limiting user sessions 54
local content 31
local subscriber database 31
location name 40
logged-in users 157
login accounts
  types 41
login name 145
login page preview 103
logo 103, 109, 114

M

MAC address 41
  of LAN device 148
manual entry 180

Downloaded from www.Manualslib.com manuals search engine

manual firmware upgrade
using TFTP 207
modulation 175
mouse action sequence syntax conventions 28
multicast pass through 55
My IP Address 62
My Subnet Mask 62

N

NAT 30, 54, 59
NAT (Network Address Translation - NAT, RFC 1631) 147
navigating 36
network cable types
100Mbps 232
10Mbps 232
networking terms glossary 27
notice message 112
notification message 121, 124

O

OFDM. See Orthogonal Frequency Division Multiplexing.
online help 27
open system 181
Orthogonal Frequency Division Multiplexing 175

P

page background 106
pass through 127
pass through list 129
password 103
payment information 121
ping command 221
Point-to-Point Tunneling Protocol 60
port mapping 147
portal page 139
post-paid 77
post-paid billing 95, 97
PPP MTU 59
PPP MTU setting 62, 63
PPPoE 30, 59, 62
PPPoE password 62
PPPoE user name 62
PPTP 30, 60, 62
PPTP password 63
PPTP server IP address 62
PPTP user name 63
preamble mode 261
preamble type 181
predefined choices 28
pre-paid 77
pre-paid billing 94
previewing printouts 114
price 114
print out time 114
printer IP address 171
printout 81
printout previews 114
private IP addresses 58
product registration 7
purchase unit 114
purchase unit message 121

Q

quick start guide 27

R

RADIUS 71, 262
shared secret key 263
RADIUS message types 262
RADIUS messages 262
redirect login page URL 68, 104
redirect subscriber login screen 104
registration
product 7
related documentation 27
replenish 81
Request To Send 177
reset button 33, 44
restart 223
restoring factory-defaults 44
restricted destination list 132
reverse SMA connectors 32
RTS (Request To Send) 260
RTS /CTS threshold 176
RTS threshold 181, 259, 260

Downloaded from www.Manualslib.com manuals search engine

S

safety warnings 6
scheduled firmware upgrade 209
screens overview 38
secret key 171
secure administrator IP addresses 54
Secure Socket Layer 211
security parameters 265
select 28
server configuration 63
server port 147
service name 62
service selection message 121
Service Set 180
session limits 54
session list 197
session trace 161
share LAN resource 136
shared key 181
SMTP port 66, 155
specifying an inside server 150
SSL 211
SSL certificate 55, 194
SSL certificate download 218
SSL login page security 68
SSL secure login 30
SSL security 65
SSL security certificate 212
SSL security for subscriber logins 217
standard subscriber login screen 102
statement printer 33, 169
static IP 62
submit button 124
subnet 267
subnet mask 58, 269
  LAN 62, 193
  WAN 62, 193
subnetting 269
subscriber accounts 79
subscriber information window 110
subscriber login 183
subscriber login screen
  advanced 105
  framed 108
  redirect 104
  standard 102
subtitle 103, 114
super subscriber account 42
supervisor account 42
supporting disk 27
syntax conventions 28
syslog 32, 153
  log settings 155
syslog server 154
system boot notice 157
system information 157, 191
system login accounts
  account manager 42
  administrator 41
system manager activity information 157
system name 49
system time 41
system up time 41
system/host name 40

T

tax 114
tax percentage 77
TCP MSS 60
TCP MSS setting 62, 63
three-buttons printer 81
time to finish 73, 77
time-to-finish accounting 75
title 103, 114
total 114
trademarks 3
troubleshooting 225

U

unit price 82
usage time 114, 124
user agreement 68, 158
user guide feedback 27
user name 103
user session limited 54
using LEDs to diagnose problems 225

V

virtual port 147, 148
VPN pass through 30

Downloaded from www.Manualslib.com manuals search engine

W

walled garden **31**, **141**
  login **142**
WAN
  IP address **41**, **62**, **193**
  MAC address **41**, **62**, **193**
  port mode **62**
  status **41**
  subnet mask **41**, **62**, **193**
  type **41**
WAN port mode **193**
warning/alarm message **112**
warranty **7**
  note **7**
web configurator **35**
  accessing **35**
  screens overview **38**
  supported browsers **35**
web configurator online help **27**
web server **65**
  port **65**
web site **27**
web-based account generator panel **81**
welcome slogan **106**
WEP **29**, **176**, **180**, **194**
WEP encryption **114**
Wi-Fi based Wireless Internet Service Provider Roaming **74**
wireless **193**
wireless association information **157**
wireless channel **41**
wireless firmware version **193**
wireless LAN **173**
  coverage **175**
wireless service **41**
wireless standards **175**
WISPr **74**
Wizard Setup **36**, **49**
WLAN **173**
  interference **259**
  security parameters **265**
WorldPay **91**
  currency code **91**
  installation ID **91**
  payment gateway **91**
  test mode **91**
WPA **29**, **176**, **180**, **194**
WPA encryption **114**

Downloaded from www.Manualslib.com manuals search engine