

# *P-660R-Tx v2 Series*

*ADSL2+ Access Router*

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

Version 3.40  
7/2006

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is lowercase and the "XEL" is uppercase.

# 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.

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

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

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

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

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

### Notice 1

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

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

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### Viewing Certifications

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

# Safety Warnings

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

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- 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.

# ZyXEL Limited Warranty

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

## Note

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

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

# Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	SUPPORT E-MAIL	TELEPHONE	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
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	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
	sales@zyxel.co.cr	+506-2015098	ftp.zyxel.co.cr	
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	

LOCATION	METHOD	SUPPORT E-MAIL	TELEPHONE	WEB SITE	REGULAR MAIL
		SALES E-MAIL	FAX	FTP SITE	
NORWAY		support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Niils Hansens vei 13 0667 Oslo Norway
		sales@zyxel.no	+47-22-80-61-81		
POLAND		info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
			+48 (22) 333 8251		
RUSSIA		http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
		sales@zyxel.ru	+7-095-542-89-25		
SPAIN		support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 Madrid Spain
		sales@zyxel.es	+34-913-005-345		
SWEDEN		support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
		sales@zyxel.se	+46-31-744-7701		
UKRAINE		support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
		sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM		support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
		sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

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

# Table of Contents

<b>Copyright</b> .....	<b>2</b>
<b>Certifications</b> .....	<b>3</b>
<b>Safety Warnings</b> .....	<b>4</b>
<b>ZyXEL Limited Warranty</b> .....	<b>5</b>
<b>Customer Support</b> .....	<b>6</b>
<b>Table of Contents</b> .....	<b>8</b>
<b>List of Figures</b> .....	<b>14</b>
<b>List of Tables</b> .....	<b>18</b>
<b>Preface</b> .....	<b>20</b>
<b>Chapter 1</b>	
<b>Getting To Know Your ZyXEL Device</b> .....	<b>22</b>
1.1 Introducing the ZyXEL Device .....	22
1.1.1 Features of the ZyXEL Device .....	22
1.2 Applications for the ZyXEL Device .....	26
1.2.1 Internet Access .....	27
1.2.2 LAN to LAN Application .....	27
1.3 ZyXEL Device Hardware Installation and Connection .....	27
1.4 Front Panel LEDs .....	28
<b>Chapter 2</b>	
<b>Introducing the Web Configurator</b> .....	<b>30</b>
2.1 Web Configurator Overview .....	30
2.1.1 Accessing the ZyXEL Device Web Configurator .....	30
2.2 Resetting the ZyXEL Device .....	31
2.2.1 Using the Reset Button .....	32
2.3 Navigating the ZyXEL Device Web Configurator .....	32
<b>Chapter 3</b>	
<b>Wizard Setup</b> .....	<b>34</b>
3.1 Introduction .....	34
3.1.1 Encapsulation .....	34
3.1.1.1 ENET ENCAP .....	34



3.1.1.2 PPP over Ethernet .....	34
3.1.1.3 PPPoA .....	34
3.1.1.4 RFC 1483 .....	35
3.1.2 Multiplexing .....	35
3.1.2.1 VC-based Multiplexing .....	35
3.1.2.2 LLC-based Multiplexing .....	35
3.1.3 VPI and VCI .....	35
3.1.4 Internet Access Wizard Setup: First Screen .....	35
3.2 IP Address and Subnet Mask .....	36
3.2.1 IP Address Assignment .....	37
3.2.1.1 IP Assignment with PPPoA or PPPoE Encapsulation .....	37
3.2.1.2 IP Assignment with RFC 1483 Encapsulation .....	37
3.2.1.3 IP Assignment with ENET ENCAP Encapsulation .....	37
3.2.1.4 Private IP Addresses .....	38
3.2.2 Nailed-Up Connection (PPP) .....	38
3.2.3 NAT .....	38
3.2.4 Internet Access Wizard Setup: Second Screen .....	38
3.2.5 DHCP Setup .....	42
3.2.5.1 IP Pool Setup .....	42
3.2.6 Internet Access Wizard Setup: Third Screen .....	42
3.2.7 Internet Access Wizard Setup: Connection Test .....	45
3.2.7.1 Test Your Internet Connection .....	45
<b>Chapter 4</b>	
<b>Password Setup .....</b>	<b>46</b>
4.1 Password Overview .....	46
4.1.1 Configuring Password .....	46
<b>Chapter 5</b>	
<b>LAN Setup .....</b>	<b>48</b>
5.1 LAN Overview .....	48
5.1.1 LANs, WANs and the ZyXEL Device .....	48
5.2 DNS Server Address .....	49
5.3 DNS Server Address Assignment .....	49
5.4 LAN TCP/IP .....	50
5.4.1 Factory LAN Defaults .....	50
5.4.2 IP Address and Subnet Mask .....	50
5.4.3 RIP Setup .....	50
5.4.4 Multicast .....	51
5.5 Any IP .....	51
5.5.1 How Any IP Works .....	52
5.6 Configuring LAN .....	53

<b>Chapter 6</b>	
<b>WAN Setup</b> .....	<b>56</b>
6.1 WAN Overview .....	56
6.2 Metric .....	56
6.3 PPPoE Encapsulation .....	57
6.4 Traffic Shaping .....	57
6.5 Zero Configuration Internet Access .....	58
6.6 Configuring WAN Setup .....	58
6.7 Traffic Redirect .....	61
6.8 Configuring WAN Backup .....	62
<b>Chapter 7</b>	
<b>Network Address Translation (NAT) Screens</b> .....	<b>66</b>
7.1 NAT Overview .....	66
7.1.1 NAT Definitions .....	66
7.1.2 What NAT Does .....	67
7.1.3 How NAT Works .....	67
7.1.4 NAT Application .....	68
7.1.5 NAT Mapping Types .....	68
7.2 SUA (Single User Account) Versus NAT .....	69
7.3 SUA Server .....	70
7.3.1 Default Server IP Address .....	70
7.3.2 Port Forwarding: Services and Port Numbers .....	70
7.3.3 Configuring Servers Behind SUA (Example) .....	71
7.4 Selecting the NAT Mode .....	71
7.5 Configuring SUA Server .....	72
7.6 Configuring Address Mapping .....	74
7.7 Editing an Address Mapping Rule .....	75
<b>Chapter 8</b>	
<b>Dynamic DNS Setup</b> .....	<b>78</b>
8.1 Dynamic DNS .....	78
8.1.1 DYNDNS Wildcard .....	78
8.2 Configuring Dynamic DNS .....	78
<b>Chapter 9</b>	
<b>Time and Date</b> .....	<b>80</b>
9.1 Configuring Time and Date .....	80
<b>Chapter 10</b>	
<b>Remote Management Configuration</b> .....	<b>82</b>
10.1 Remote Management Overview .....	82
10.1.1 Remote Management Limitations .....	82

10.1.2 Remote Management and NAT .....	83
10.1.3 System Timeout .....	83
10.2 Telnet .....	83
10.3 FTP .....	83
10.4 Web .....	83
10.5 Configuring Remote Management .....	83
<b>Chapter 11</b>	
<b>Universal Plug-and-Play (UPnP) .....</b>	<b>86</b>
11.1.1 How do I know if I'm using UPnP? .....	86
11.1.2 NAT Traversal .....	86
11.1.3 Cautions with UPnP .....	87
11.2 UPnP and ZyXEL .....	87
11.2.1 Configuring UPnP .....	87
11.3 Installing UPnP in Windows Example .....	88
11.4 Using UPnP in Windows XP Example .....	92
<b>Chapter 12</b>	
<b>Maintenance .....</b>	<b>98</b>
12.1 Maintenance Overview .....	98
12.2 System Status Screen .....	98
12.2.1 System Statistics .....	100
12.3 DHCP Table Screen .....	101
12.4 Any IP Table Screen .....	102
12.5 Diagnostic Screens .....	103
12.5.1 Diagnostic General Screen .....	103
12.5.2 Diagnostic DSL Line Screen .....	104
12.6 Firmware Screen .....	105
12.7.1 Backup Configuration .....	107
12.7.2 Restore Configuration .....	108
12.7.3 Back to Factory Defaults .....	109
<b>Chapter 13</b>	
<b>Troubleshooting .....</b>	<b>112</b>
13.1 Problems Starting Up the ZyXEL Device .....	112
13.2 Problems with the LAN LED .....	112
13.3 Problems with the Password .....	113
13.4 Problems with the DSL LED .....	113
13.5 Problems with the LAN Interface .....	113
13.6 Problems with the WAN Interface .....	114
13.7 Problems with Internet Access .....	114
13.8 Problems with Remote Management .....	114
13.9 Problems with the Web Configurator .....	115

13.9.1 Pop-up Windows, JavaScripts and Java Permissions .....	115
13.9.1.1 Internet Explorer Pop-up Blockers .....	115
13.9.1.2 JavaScripts .....	118
13.9.1.3 Java Permissions .....	120
<b>Appendix A</b>	
<b>Product Specifications .....</b>	<b>124</b>
<b>Appendix B</b>	
<b>Setting up Your Computer's IP Address.....</b>	<b>128</b>
Windows 95/98/Me.....	128
Installing Components .....	129
Configuring .....	130
Verifying Settings.....	131
Windows 2000/NT/XP .....	131
Verifying Settings.....	136
Macintosh OS 8/9.....	136
Verifying Settings.....	138
Macintosh OS X .....	138
Verifying Settings.....	139
Linux.....	139
Using the K Desktop Environment (KDE).....	140
Using Configuration Files.....	141
Verifying Settings.....	143
<b>Appendix C</b>	
<b>IP Addresses and Subnetting .....</b>	<b>144</b>
Introduction to IP Addresses.....	144
IP Address Classes and Hosts .....	144
Subnet Masks .....	146
Subnetting.....	146
Example: Two Subnets .....	147
Example: Four Subnets.....	148
Example Eight Subnets.....	149
Subnetting With Class A and Class B Networks .....	150
<b>Appendix D</b>	
<b>Splitters and Microfilters .....</b>	<b>152</b>
Connecting a POTS Splitter .....	152
Telephone Microfilters .....	152
ZyXEL Device With ISDN.....	153
<b>Appendix E</b>	

<b>Command Interpreter</b> .....	<b>156</b>
Command Syntax.....	156
Command Usage .....	156
<b>Appendix F</b>	
<b>Log Descriptions</b> .....	<b>158</b>
<b>Appendix G</b>	
<b>PPPoE</b> .....	<b>162</b>
PPPoE in Action.....	162
Benefits of PPPoE.....	162
Traditional Dial-up Scenario .....	162
How PPPoE Works .....	163
ZyXEL Device as a PPPoE Client.....	163
<b>Appendix H</b>	
<b>Virtual Circuit Topology</b> .....	<b>164</b>
<b>Index</b> .....	<b>166</b>

# List of Figures

Figure 1 ZyXEL Device Internet Access Application .....	27
Figure 2 ZyXEL Device LAN-to-LAN Application .....	27
Figure 3 Password Screen .....	31
Figure 4 Change Password at Login .....	31
Figure 5 Web Configurator: Site Map Screen .....	32
Figure 6 Internet Access Wizard Setup: First Screen .....	36
Figure 7 Internet Connection with PPPoE .....	39
Figure 8 Internet Connection with RFC 1483 .....	40
Figure 9 Internet Connection with ENET ENCAP .....	40
Figure 10 Internet Connection with PPPoA .....	41
Figure 11 Internet Access Wizard Setup: Third Screen .....	43
Figure 12 Internet Access Wizard Setup: LAN Configuration .....	44
Figure 13 Internet Access Wizard Setup: Connection Tests .....	45
Figure 14 Password .....	46
Figure 15 LAN and WAN IP Addresses .....	48
Figure 16 Any IP Example .....	52
Figure 17 LAN Setup .....	53
Figure 18 Example of Traffic Shaping .....	58
Figure 19 WAN Setup (PPPoE) .....	59
Figure 20 Traffic Redirect Example .....	62
Figure 21 Traffic Redirect LAN Setup .....	62
Figure 22 WAN Backup .....	63
Figure 23 How NAT Works .....	68
Figure 24 NAT Application With IP Alias .....	68
Figure 25 Multiple Servers Behind NAT Example .....	71
Figure 26 NAT Mode .....	72
Figure 27 Edit SUA/NAT Server Set .....	73
Figure 28 Address Mapping Rules .....	74
Figure 29 Address Mapping Rule Edit .....	75
Figure 30 Dynamic DNS .....	79
Figure 31 Time and Date .....	80
Figure 32 Telnet Configuration on a TCP/IP Network .....	83
Figure 33 Remote Management .....	84
Figure 34 Configuring UPnP .....	88
Figure 35 Add/Remove Programs: Windows Setup: Communication .....	89
Figure 36 Add/Remove Programs: Windows Setup: Communication: Components .....	89
Figure 37 Network Connections .....	90
Figure 38 Windows Optional Networking Components Wizard .....	91

Figure 39 Networking Services .....	91
Figure 40 Network Connections .....	92
Figure 41 Internet Connection Properties .....	93
Figure 42 Internet Connection Properties: Advanced Settings .....	94
Figure 43 Internet Connection Properties: Advanced Settings: Add .....	94
Figure 44 System Tray Icon .....	95
Figure 45 Internet Connection Status .....	95
Figure 46 Network Connections .....	96
Figure 47 Network Connections: My Network Places .....	97
Figure 48 Network Connections: My Network Places: Properties: Example .....	97
Figure 49 System Status .....	99
Figure 50 System Status: Show Statistics .....	100
Figure 51 DHCP Table .....	102
Figure 52 Any IP Table .....	102
Figure 53 Diagnostic: General .....	103
Figure 54 Diagnostic: DSL Line .....	104
Figure 55 Firmware Upgrade .....	106
Figure 56 Network Temporarily Disconnected .....	106
Figure 57 Error Message .....	107
Figure 58 Configuration .....	107
Figure 59 Backup Configuration .....	108
Figure 60 Restore Configuration .....	108
Figure 61 Restore Configuration Successful .....	109
Figure 62 Network Temporarily Disconnected .....	109
Figure 63 Reset to Factory Default Settings .....	110
Figure 64 Pop-up Blocker .....	116
Figure 65 Internet Options .....	116
Figure 66 Internet Options .....	117
Figure 67 Pop-up Blocker Settings .....	118
Figure 68 Internet Options .....	119
Figure 69 Security Settings - Java Scripting .....	120
Figure 70 Security Settings - Java .....	121
Figure 71 Java (Sun) .....	122
Figure 72 Windows 95/98/Me: Network: Configuration .....	129
Figure 73 Windows 95/98/Me: TCP/IP Properties: IP Address .....	130
Figure 74 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	131
Figure 75 Windows XP: Start Menu .....	132
Figure 76 Windows XP: Control Panel .....	132
Figure 77 Windows XP: Control Panel: Network Connections: Properties .....	133
Figure 78 Windows XP: Local Area Connection Properties .....	133
Figure 79 Windows XP: Internet Protocol (TCP/IP) Properties .....	134
Figure 80 Windows XP: Advanced TCP/IP Properties .....	135
Figure 81 Windows XP: Internet Protocol (TCP/IP) Properties .....	136

---

Figure 82 Macintosh OS 8/9: Apple Menu .....	137
Figure 83 Macintosh OS 8/9: TCP/IP .....	137
Figure 84 Macintosh OS X: Apple Menu .....	138
Figure 85 Macintosh OS X: Network .....	139
Figure 86 Red Hat 9.0: KDE: Network Configuration: Devices .....	140
Figure 87 Red Hat 9.0: KDE: Ethernet Device: General .....	140
Figure 88 Red Hat 9.0: KDE: Network Configuration: DNS .....	141
Figure 89 Red Hat 9.0: KDE: Network Configuration: Activate .....	141
Figure 90 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .....	142
Figure 91 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .....	142
Figure 92 Red Hat 9.0: DNS Settings in resolv.conf .....	142
Figure 93 Red Hat 9.0: Restart Ethernet Card .....	143
Figure 94 Red Hat 9.0: Checking TCP/IP Properties .....	143
Figure 95 Connecting a POTS Splitter .....	152
Figure 96 Connecting a Microfilter .....	153
Figure 97 ZyXEL Device with ISDN .....	154
Figure 98 Single-Computer per Router Hardware Configuration .....	163
Figure 99 ZyXEL Device as a PPPoE Client .....	163
Figure 100 Virtual Circuit Topology .....	164





# List of Tables

Table 1 ADSL Standards .....	22
Table 2 Front Panel LED Description .....	28
Table 3 Web Configurator Screens Summary .....	32
Table 4 Internet Access Wizard Setup: First Screen .....	36
Table 5 Internet Connection with PPPoE .....	39
Table 6 Internet Connection with RFC 1483 .....	40
Table 7 Internet Connection with ENET ENCAP .....	41
Table 8 Internet Connection with PPPoA .....	42
Table 9 Internet Access Wizard Setup: LAN Configuration .....	44
Table 10 Password .....	46
Table 11 LAN Setup .....	53
Table 12 WAN Setup .....	59
Table 13 WAN Backup .....	63
Table 14 NAT Definitions .....	66
Table 15 NAT Mapping Types .....	69
Table 16 Services and Port Numbers .....	70
Table 17 NAT Mode .....	72
Table 18 Edit SUA/NAT Server Set .....	73
Table 19 Address Mapping Rules .....	74
Table 20 Address Mapping Rule Edit .....	76
Table 21 Dynamic DNS .....	79
Table 22 Time and Date .....	81
Table 23 Remote Management .....	84
Table 24 Configuring UPnP .....	88
Table 25 System Status .....	99
Table 26 System Status: Show Statistics .....	101
Table 27 DHCP Table .....	102
Table 28 Any IP Table .....	102
Table 29 Diagnostic: General .....	104
Table 30 Diagnostic: DSL Line .....	105
Table 31 Firmware Upgrade .....	106
Table 32 Backup Configuration .....	108
Table 33 Maintenance Restore Configuration .....	108
Table 34 Troubleshooting the Start-Up of Your ZyxEL Device .....	112
Table 35 Troubleshooting the LAN LED .....	112
Table 36 Troubleshooting the Password .....	113
Table 37 Troubleshooting the DSL LED .....	113
Table 38 Troubleshooting the LAN Interface .....	113

Table 39 Troubleshooting the WAN Interface .....	114
Table 40 Troubleshooting Internet Access .....	114
Table 41 Troubleshooting Remote Management .....	114
Table 42 Troubleshooting the Web Configurator .....	115
Table 43 Device .....	124
Table 44 Firmware .....	125
Table 45 Classes of IP Addresses .....	145
Table 46 Allowed IP Address Range By Class .....	145
Table 47 "Natural" Masks .....	146
Table 48 Alternative Subnet Mask Notation .....	146
Table 49 Two Subnets Example .....	147
Table 50 Subnet 1 .....	147
Table 51 Subnet 2 .....	148
Table 52 Subnet 1 .....	148
Table 53 Subnet 2 .....	149
Table 54 Subnet 3 .....	149
Table 55 Subnet 4 .....	149
Table 56 Eight Subnets .....	150
Table 57 Class C Subnet Planning .....	150
Table 58 Class B Subnet Planning .....	151
Table 59 System Maintenance Logs .....	158
Table 60 System Error Logs .....	159
Table 61 Packet Filter Logs .....	159
Table 62 CDR Logs .....	159
Table 63 PPP Logs .....	160
Table 64 ICMP Notes .....	160

# Preface

Congratulations on your purchase of the P-660R-Tx v2 ADSL2+ Access Router.

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

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.

Use the web configurator or command interpreter interface to configure your ZyXEL Device. Not all features can be configured through all interfaces.

## 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”.
- The P-660R-Tx v2 series may be referred to as “the ZyXEL Device” in this user’s guide. This refers to both models (ADSL over POTS and ADSL over ISDN) unless specifically identified.









## 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 connection information and instructions on getting started.
- Web Configurator Online Help  
Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Glossary and Web Site  
Please refer to [www.zyxel.com](http://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](mailto:techwriters@zyxel.com.tw) or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

## Graphics Icons Key

ZyXEL Device 	Computer 	Notebook computer 
Server 	DSLAM 	Telephone 
Router 	Switch 	

# CHAPTER 1

## Getting To Know Your ZyXEL Device

This chapter describes the key features and applications of your ZyXEL Device.

### 1.1 Introducing the ZyXEL Device

Your ZyXEL Device integrates a high-speed 10/100Mbps auto-negotiating LAN interface and a high-speed ADSL port into a single package.

Models ending in "1", for example P-660R-T1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Synchronous Digital System). Models ending in "7" denote a device that works over T-ISDN (UR-2).

**Note:** Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

The web browser-based Graphical User Interface (GUI) provides easy management.

#### 1.1.1 Features of the ZyXEL Device

The following sections describe the features of the ZyXEL Device.

##### High Speed Internet Access

The ZyXEL Device is an ADSL router compatible with the ADSL/ADSL2/ADSL2+ standards. It allows super-fast, secure Internet access over the analog (POTS) or digital (ISDN) telephone line (depending on your model). Maximum data rates attainable for each standard are shown in the next table.

**Table 1** ADSL Standards

DATARATE STANDARD	UPSTREAM	DOWNSTREAM
ADSL	832 kbps	8Mbps
ADSL2	3.5Mbps	12Mbps
ADSL2+	3.5Mbps	24Mbps

**Note:** If your ZyXEL Device does not support Annex M, the maximum ADSL2/2+ upstream data rate is 1.2 Mbps. ZyXEL Devices which work over ISDN do not support Annex M.

The standard your ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, line quality, etc.

## **Zero Configuration Internet Access**

Once you connect and turn on the ZyXEL Device, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the ZyXEL Device cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.

## **Any IP**

The Any IP feature allows a computer to access the Internet and the ZyXEL Device 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.

## **Traffic Redirect**

Traffic redirect forwards WAN traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet, thus acting as an auxiliary if your regular WAN connection fails.

## **Universal Plug and Play (UPnP)**

Using the standard TCP/IP protocol, the ZyXEL Device and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

## **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)**

Network Address Translation (NAT) allows the translation of an Internet protocol address 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).

## **10/100M Auto-negotiating Ethernet/Fast Ethernet Interface(s)**

This auto-negotiation 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.

## **Auto-Crossover (MDI/MDI-X) 10/100 Mbps Ethernet Interface(s)**

These interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

## **Dynamic DNS Support**

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

## **Multiple PVC (Permanent Virtual Circuits) Support**

Your ZyXEL Device supports up to 8 PVC's.

## **ADSL Standards**

- Full-Rate (ANSI T1.413, Issue 2; G.dmt (G.992.1) with line rate support of up to 8 Mbps downstream and 832 Kbps upstream.
- G.lite (G.992.2) with line rate support of up to 1.5Mbps downstream and 512Kbps upstream.
- Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G.992.2)).
- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- ATM Forum UNI 3.1/4.0 PVC.
- Supports up to 8 PVCs (UBR, CBR, VBR).
- Multiple Protocol over AAL5 (RFC 1483).
- PPP over AAL5 (RFC 2364).
- PPP over Ethernet over AAL5 (RFC 2516).
- RFC 1661.
- PPP over PAP (RFC 1334).
- PPP over CHAP (RFC 1994).

## **Protocol Support**

- DHCP Support

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



- IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

- IP Policy Routing (IPPR)

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

- PPP (Point-to-Point Protocol) link layer protocol.
- Transparent bridging for unsupported network layer protocols.
- RIP I/RIP II
- IGMP Proxy
- ICMP support
- ATM QoS support
- MIB II support (RFC 1213)

## **Networking Compatibility**

Your ZyXEL Device is compatible with the major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers, making configuration as simple as possible for you.

## **Multiplexing**

The ZyXEL Device supports VC-based and LLC-based multiplexing.

## **Encapsulation**

The ZyXEL Device supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM, MAC encapsulated routing (ENET encapsulation) as well as PPP over Ethernet (RFC 2516).

## **Network Management**

- Embedded web configurator
- CLI (Command Line Interpreter)
- Remote Management via Telnet or Web
- SNMP manageable
- DHCP Server/Client/Relay
- Built-in Diagnostic Tools
- Syslog
- Telnet Support (Password-protected telnet access to internal configuration manager)
- TFTP/FTP server, firmware upgrade and configuration backup/support supported

- Supports OAM F4/F5 loop-back, AIS and RDI OAM cells

### **Other PPPoE Features**

- PPPoE idle time out
- PPPoE Dial on Demand

### **Diagnostics Capabilities**

The ZyXEL Device can perform self-diagnostic tests. These tests check the integrity of the following circuitry:

- FLASH memory
- ADSL circuitry
- RAM
- LAN port

### **Packet Filters**

The ZyXEL Device's packet filtering functions allows added network security and management.

### **Ease of Installation**

Your ZyXEL Device is designed for quick, intuitive and easy installation.

### **Housing**

Your ZyXEL Device's compact and ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

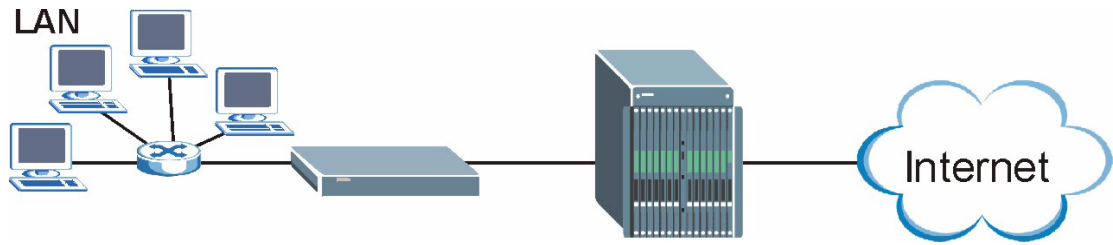
## **1.2 Applications for the ZyXEL Device**

Here are some example uses for which the ZyXEL Device is well suited.

### **1.2.1 Internet Access**

The ZyXEL Device is the ideal high-speed Internet access solution. Your ZyXEL Device supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers. A DSLAM is a rack of ADSL line cards with data multiplexed into a backbone network interface/connection (for example, T1, OC3, DS3, ATM or Frame Relay). Think of it as the equivalent of a modem rack for ADSL. A typical Internet access application is shown below.

**Figure 1** ZyXEL Device Internet Access Application



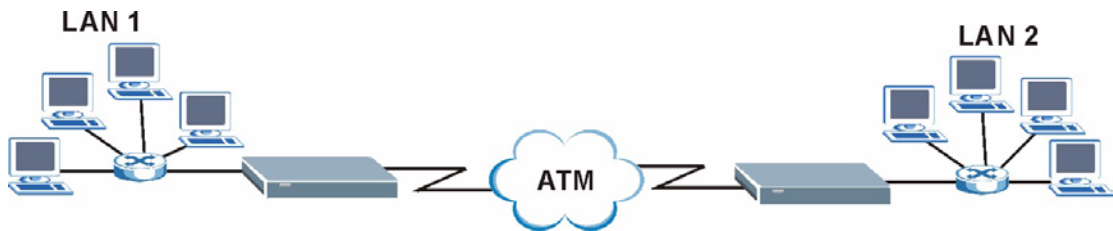
**Internet Single User Account**

For a SOHO (Small Office/Home Office) environment, your ZyXEL Device offers the Single User Account (SUA) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single IP address.

**1.2.2 LAN to LAN Application**

You can use the ZyXEL Device to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application for your ZyXEL Device is shown as follows.

**Figure 2** ZyXEL Device LAN-to-LAN Application



**1.3 ZyXEL Device Hardware Installation and Connection**

Refer to the Quick Start Guide for information on hardware installation and connection.

**1.4 Front Panel LEDs**

The following table describes the LEDs on the front panel.

**Table 2** Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting.
		Off	The ZyXEL Device is not ready or has malfunctioned.
	Red	On	The power to the ZyXEL Device is too low.

**Table 2** Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
10/100M	Green	On	The ZyXEL Device has a successful 10Mbps Ethernet connection.
		Blinking	The ZyXEL Device is receiving or sending data.
	Amber	On	The ZyXEL Device has a successful 100Mbps Ethernet connection.
		Blinking	The ZyXEL Device is receiving or sending data.
		Off	The LAN is not connected.
DSL	Green	On	The ZyXEL Device is linked successfully to a DSLAM.
		Blinking (Slow)	The ZyXEL Device is initializing the DSL line.
		Blinking (Fast)	The ZyXEL Device is sending or receiving non-PPP traffic.
		Off	The DSL link is down.
PPP	Amber	On	The ZyXEL Device has a PPP (PPPoA or PPPoE) connection.
		Blinking	The ZyXEL Device is sending or receiving PPPoA or PPPoE traffic.
		Off	The ZyXEL Device does not have a PPP (PPPoA or PPPoE) connection.



# CHAPTER 2

## Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

### 2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyXEL Device setup and management via an Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

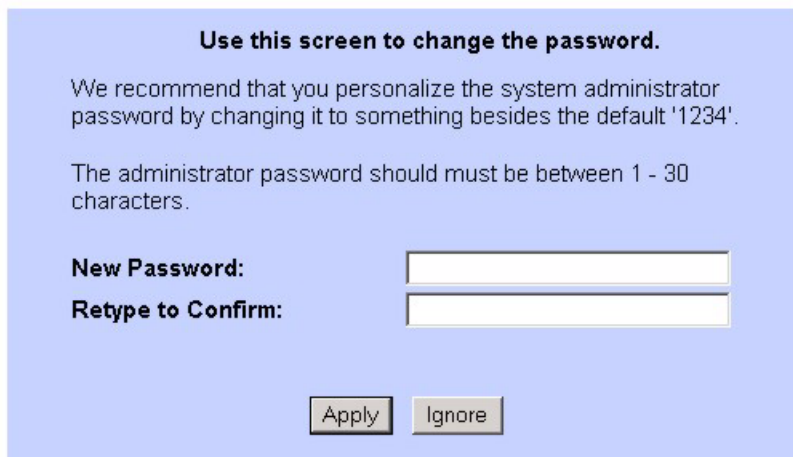
#### 2.1.1 Accessing the ZyXEL Device Web Configurator

- 1** Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
- 2** Prepare your computer/computer network to connect to the ZyXEL Device (refer to [Appendix B on page 128](#)).
- 3** Launch your web browser.
- 4** Type "192.168.1.1" as the URL.
- 5** An **Enter Network Password** window displays. Enter the password ("1234" is the default). Click **Login** to proceed to a screen asking you to change your password. Click **Cancel** to revert to the default password in the password field.

**Figure 3** Password Screen

- 6** It is highly recommended you change the default password! Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

**Note:** If you do not change the password, the following screen appears every time you log in.

**Figure 4** Change Password at Login

- 7** You should now see the **SITE MAP** screen.

**Note:** The ZyXEL Device automatically times out after five minutes of inactivity. Simply log back into the ZyXEL Device if this happens to you.

## 2.2 Resetting the ZyXEL Device

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the ZyXEL Device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

## 2.2.1 Using the Reset Button

- 1 Make sure the **PWR/SYS** LED is on (not blinking).
- 2 Press the **RESET** button for ten seconds or until the **PWR/SYS** LED begins to blink and then release it. When the **PWR/SYS** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts.

## 2.3 Navigating the ZyXEL Device Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen.

- Click **Wizard Setup** to begin a series of screens to configure your ZyXEL Device for the first time.
- Click a link under **Advanced Setup** to configure advanced ZyXEL Device features.
- Click a link under **Maintenance** to see ZyXEL Device performance statistics, upload firmware and back up, restore or upload a configuration file.
- Click **SITE MAP** to go to the **Site Map** screen.
- Click **Logout** in the navigation panel when you have finished a ZyXEL Device management session.

**Figure 5** Web Configurator: Site Map Screen



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

**Table 3** Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup	Connection Setup	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
Advanced Setup		
Password		Use this screen to change your password.
LAN		Use this screen to configure LAN DHCP and TCP/IP settings.



**Table 3** Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
WAN	WAN Setup	Use this screen to change the ZyXEL Device's WAN remote node settings.
	WAN Backup	Use this screen to configure your traffic redirect properties and WAN backup settings.
NAT	SUA Only	Use this screen to configure servers behind the ZyXEL Device.
	Full Feature	Use this screen to configure network address translation mapping rules.
Security		Use this screen to configure Internet security and apply the predefined filter rules.
Dynamic DNS		Use this screen to set up dynamic DNS.
Time and Date		Use this screen to change your ZyXEL Device's time and date.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the ZyXEL Device.
UPnP		Use this screen to enable UPnP on the ZyXEL Device.
Maintenance		
System Status		This screen contains administrative and system-related information.
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
Any IP Table		This screen shows current read-only information of all network devices that use the Any IP feature to communicate with the ZyXEL Device.
Diagnostic	General	These screens display information to help you identify problems with the ZyXEL Device general connection.
	DSL Line	These screens display information to help you identify problems with the DSL line.
Firmware		Use this screen to upload firmware to your ZyXEL Device.
Configuration		This screen is only available on the P-660R-T1C v2. Use these screens to backup, restore or reset the configuration of your ZyXEL Device.
LOGOUT		Click this label to exit the web configurator.

# CHAPTER 3

## Wizard Setup

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

### 3.1 Introduction

Use the **Wizard Setup** screens to configure your system for Internet access with the information provided by your ISP. Your ISP may have already configured some of the fields in the wizard screens for you.

#### 3.1.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device supports the following methods.

##### 3.1.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **ENET ENCAP Gateway** field in the second wizard screen. You can get this information from your ISP.

##### 3.1.1.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The ZyXEL Device bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendices.

##### 3.1.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

### **3.1.1.4 RFC 1483**

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

## **3.1.2 Multiplexing**

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

### **3.1.2.1 VC-based Multiplexing**

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

### **3.1.2.2 LLC-based Multiplexing**

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

## **3.1.3 VPI and VCI**

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

## **3.1.4 Internet Access Wizard Setup: First Screen**

In the **SITE MAP** screen click **Wizard Setup** to display the first wizard screen.

**Figure 6** Internet Access Wizard Setup: First Screen

The following table describes the labels in this screen.

**Table 4** Internet Access Wizard Setup: First Screen

LABEL	DESCRIPTION
Mode	From the <b>Mode</b> drop-down list box, select <b>Routing</b> (default) if your ISP allows multiple computers to share an Internet account. Otherwise select <b>Bridge</b> .
Encapsulation	Select the encapsulation type your ISP uses from the <b>Encapsulation</b> drop-down list box. Choices vary depending on what you select in the <b>Mode</b> field. If you select <b>Bridge</b> in the <b>Mode</b> field, select either <b>PPPoA</b> or <b>RFC 1483</b> . If you select <b>Routing</b> in the <b>Mode</b> field, select <b>PPPoA</b> , <b>RFC 1483</b> , <b>ENET ENCAP</b> or <b>PPPoE</b> .
Multiplex	Select the multiplexing method used by your ISP from the <b>Multiplex</b> drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Next	Click this button to go to the next wizard screen. The next wizard screen you see depends on what protocol you chose above. Click on the protocol link to see the next wizard screen for that protocol.

## 3.2 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

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

### 3.2.1 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

#### 3.2.1.1 IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the **IP Address** field and *not* the **ENET ENCAP Gateway** field.

#### 3.2.1.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the **IP Address** and **ENET ENCAP Gateway** fields as stated above.

#### 3.2.1.3 IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **ENET ENCAP Gateway** fields as supplied by your ISP. However for a dynamic IP, the ZyXEL Device acts as a DHCP client on the WAN port and so the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A) as the DHCP server assigns them to the ZyXEL Device.

### 3.2.1.4 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.

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

### 3.2.2 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyXEL Device does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyXEL Device will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern

### 3.2.3 NAT

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 to a different IP address known within another network.

### 3.2.4 Internet Access Wizard Setup: Second Screen

The second wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

**Figure 7** Internet Connection with PPPoE

**Wizard Setup - ISP Parameters for Internet Access**

Service Name

User Name

Password

**IP Address**

Obtain an IP Address Automatically

Static IP Address

**Connection**

Connect on Demand: Max Idle Timeout  sec

Nailed-Up Connection

**Network Address Translation**

▼

The following table describes the labels in this screen.

**Table 5** Internet Connection with PPPoE

LABEL	DESCRIPTION
Service Name	Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form <a href="#">user@domain</a> where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the text box below.
Connection	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out (in seconds) in the <b>Max. Idle Timeout</b> field. The default setting selects <b>Connection on Demand</b> with 0 as the idle time-out, which means the Internet session will not timeout. Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Network Address Translation	Select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> from the drop-down list box. Refer to the NAT chapter for more details.
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

**Figure 8** Internet Connection with RFC 1483

*Connection Setup- ISP Parameters for Internet Access*

---

IP Address

**Network Address Translation**  
 ▾

---

The following table describes the labels in this screen.

**Table 6** Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select <b>Routing</b> in the <b>Mode</b> field. Type your ISP assigned IP address in this field.
Network Address Translation	Select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> from the drop-down list box. Refer to <a href="#">Chapter 7 on page 66</a> for more details.
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

**Figure 9** Internet Connection with ENET ENCAP

*Connection Setup- ISP Parameters for Internet Access*

---

**IP Address**

Obtain an IP Address Automatically

Static IP Address

IP Address

Subnet Mask

ENET ENCAP Gateway

**Network Address Translation**  
 ▾

---



The following table describes the labels in this screen.

**Table 7** Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the IP Address text box below.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to <a href="#">Appendix C on page 144</a> to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway	You must specify a gateway IP address (supplied by your ISP) when you use <b>ENET ENCAP</b> in the <b>Encapsulation</b> field in the previous screen.
Network Address Translation	Select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> from the drop-down list box. Refer to the NAT chapter for more details.
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

**Figure 10** Internet Connection with PPPoA

*Connection Setup- ISP Parameters for Internet Access*

User Name:

Password:

**IP Address**

Obtain an IP Address Automatical  
 Static IP Address

**Connection**

Connect on Demand: Max Idle Tir

The following table describes the labels in this screen.

**Table 8** Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
IP Address	<p>This option is available if you select <b>Routing</b> in the <b>Mode</b> field.</p> <p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.</p> <p>Click <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise click <b>Static IP Address</b> and type your ISP assigned IP address in the IP Address text box below.</p>
Connection	<p>Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out (in seconds) in the <b>Max. Idle Timeout</b> field. The default setting selects <b>Connection on Demand</b> with 0 as the idle time-out, which means the Internet session will not timeout.</p> <p>Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.</p>
Network Address Translation	<p>This option is available if you select <b>Routing</b> in the <b>Mode</b> field.</p> <p>Select <b>None</b>, <b>SUA Only</b> or <b>Full Feature</b> from the drop-down list box. Refer to <a href="#">Chapter 7 on page 66</a> for more details.</p>
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

## 3.2.5 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

### 3.2.5.1 IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

## 3.2.6 Internet Access Wizard Setup: Third Screen

Verify the settings in the screen shown next. To change the LAN information on the ZyXEL Device, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration and skip to the section 3.13.

**Figure 11** Internet Access Wizard Setup: Third Screen

*Wizard Setup - ISP Parameters for Internet Access*

---

**WAN Information:**  
Mode: **Routing**  
Encapsulation: **PPPoE**  
Multiplexing: **LLC**  
VPI/VCI: **8/35**  
Service Name :  
User Name : **user@icp.ch**  
Password : **\*\*\*\*\***  
IP Address : **Obtain an IP Address Automatically**  
Network Address Translation: **SUA Only**  
Connect on Demand: **Max Idle Timeout 0 sec.**

**LAN Information:**  
IP Address: **192.168.1.1**  
IP Mask: **255.255.255.0**  
DHCP: **ON**  
Client IP Pool Starting Address: **192.168.1.33**  
Size of Client IP Pool: **32**

---

If you want to change your ZyXEL Device LAN settings, click **Change LAN Configuration** to display the screen as shown next.

**Figure 12** Internet Access Wizard Setup: LAN Configuration

*Connection Setup- ISP Parameters for Internet Access*

---

LAN IP Address

LAN Subnet Mask

**DHCP**

DHCP Server

Client IP Pool Starting Address

Size of Client IP Pool

Primary DNS Server

Secondary DNS Server

---

The following table describes the labels in this screen.

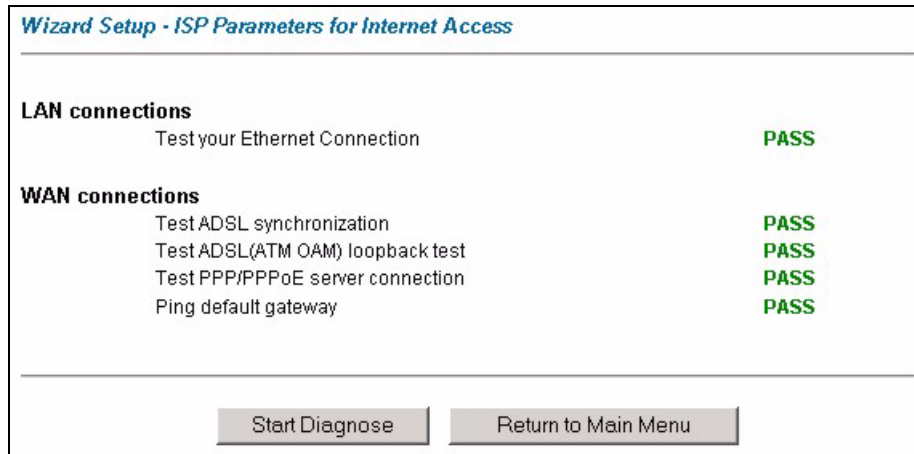
**Table 9** Internet Access Wizard Setup: LAN Configuration

LABEL	DESCRIPTION
LAN IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).  <b>Note:</b> If you changed the ZyXEL Device's LAN IP address, you must use the new IP address if you want to access the web configurator again.
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	
DHCP Server	From the <b>DHCP Server</b> drop-down list box, select <b>On</b> to allow your ZyXEL Device to assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client. Select <b>Off</b> to disable DHCP server. When DHCP server is used, set the following items:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Back	Click <b>Back</b> to go back to the previous screen.
Finish	Click <b>Finish</b> to save the settings and proceed to the next wizard screen.

## 3.2.7 Internet Access Wizard Setup: Connection Test

The ZyXEL Device automatically tests the connection to the computer(s) connected to the LAN ports. To test the connection from the ZyXEL Device to the ISP, click **Start Diagnose**. Otherwise click **Return to Main Menu** to go back to the **Site Map** screen.

**Figure 13** Internet Access Wizard Setup: Connection Tests



### 3.2.7.1 Test Your Internet Connection

Launch your web browser and navigate to [www.zyxel.com](http://www.zyxel.com). Internet access is just the beginning. Refer to the rest of this User's Guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the Wizard Setup are correct.

# CHAPTER 4

## Password Setup

This chapter provides information on the **Password** screen.

### 4.1 Password Overview

It is highly recommended that you change the password for accessing the ZyXEL Device.

#### 4.1.1 Configuring Password

To change your ZyXEL Device's password (recommended), click **Password** in the **Site Map** screen. The screen appears as shown.

**Figure 14** Password

**Password**

Old Password

New Password

Retype to confirm

**Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.**

The following table describes the fields in this screen.

**Table 10** Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 5

## LAN Setup

This chapter describes how to configure LAN settings.

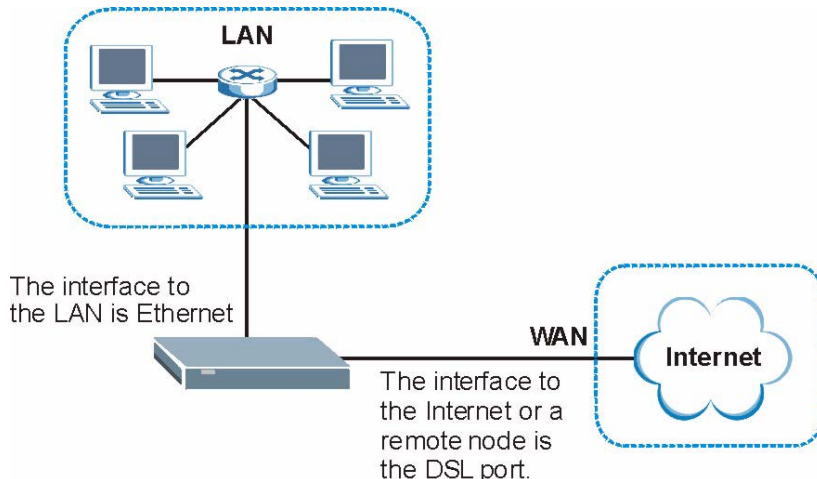
### 5.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

#### 5.1.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

**Figure 15** LAN and WAN IP Addresses





## 5.2 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. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in the **LAN Setup** screen, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in the **LAN Setup** screen are not specified, for instance, left as 0.0.0.0, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen. This way, the ZyXEL Device can pass the DNS servers to the computers and the computers can query the DNS server directly without the ZyXEL Device's intervention.

## 5.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map 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 computer before you can access it.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in the **LAN Setup** screen.
- The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left blank in the **LAN Setup** screen.

## 5.4 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

### 5.4.1 Factory LAN Defaults

The LAN parameters of the ZyXEL Device are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

### 5.4.2 IP Address and Subnet Mask

Refer to [Section 3.2 on page 36](#) in [Chapter 3 on page 34](#) for this information.

### 5.4.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None** - the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

## 5.4.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

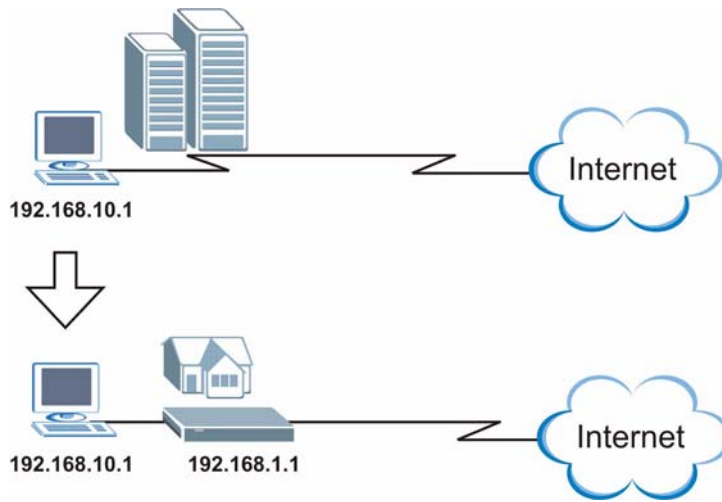
The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

## 5.5 Any IP

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.

With the Any IP 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. 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 16** Any IP Example

The Any IP 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.

**Note:** You *must* enable NAT/SUA to use the Any IP feature on the ZyXEL Device.

### 5.5.1 How Any IP 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.
- 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.

## 5.6 Configuring LAN

Click **LAN** and **LAN Setup** to open the following screen.

**Figure 17** LAN Setup

The following table describes the labels in this screen.

**Table 11** LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	<p>If set to <b>Server</b>, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to <b>None</b>, the DHCP server will be disabled.</p> <p>If set to <b>Relay</b>, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the <b>Remote DHCP Server</b> field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>

**Table 11** LAN Setup (continued)

LABEL	DESCRIPTION
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If <b>Relay</b> is selected in the <b>DHCP</b> field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.
Any IP Setup	<p>Select the <b>Active</b> checkbox to enable the Any IP 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.</p> <p>When you disable the Any IP 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.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 6

## WAN Setup

This chapter describes how to configure WAN settings.

### 6.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

See [Chapter 3 on page 34](#) for more information on the fields in the WAN screens.

### 6.2 Metric

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the ZyXEL Device's routes to the Internet. If any two of the default routes have the same metric, the ZyXEL Device uses the following pre-defined priorities:

- Normal route: designated by the ISP (see [Section 6.5 on page 58](#))
- Traffic-redirect route (see [Section 6.7 on page 61](#))
- WAN-backup route, also called dial-backup (see [Section 6.8 on page 62](#))

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyXEL Device tries the traffic-redirect route next. In the same manner, the ZyXEL Device uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

**Note:** IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above (see [Chapter 28 on page 232](#)).



## 6.3 PPPoE Encapsulation

The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

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

One of the benefits of PPPoE is the ability to let you 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 individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer 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 LANs' computers will have access.

## 6.4 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

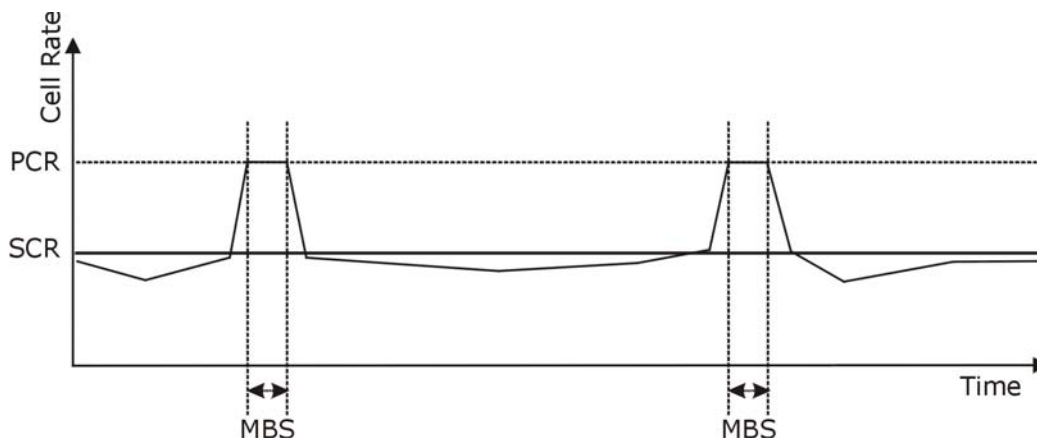
Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

**Figure 18** Example of Traffic Shaping

## 6.5 Zero Configuration Internet Access

Once you turn on and connect the ZyXEL Device to a telephone jack, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the ZyXEL Device cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.

Zero configuration for Internet access is disable when

- the ZyXEL Device is in bridge mode
- you set the ZyXEL Device to use a static (fixed) WAN IP address.

## 6.6 Configuring WAN Setup

To change your ZyXEL Device's WAN remote node settings, click **WAN** and **WAN Setup**. The screen differs by the encapsulation.

Figure 19 WAN Setup (PPPoE)

### WAN - WAN Setup

---

**Name**

**Mode**

**Encapsulation**

**Multiplex**

**Virtual Circuit ID**

VPI

VCI

**ATM QoS Type**

**Cell Rate**

Peak Cell Rate  cell/sec

Sustain Cell Rate  cell/sec

Maximum Burst Size

**Login Information**

Service Name

User Name

Password

**IP Address**

Obtain an IP Address Automatically

The following table describes the labels in this screen.

Table 12 WAN Setup

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select <b>Routing</b> (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select <b>Bridge</b> .

**Table 12** WAN Setup (continued)

LABEL	DESCRIPTION
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the <b>Mode</b> field. If you select <b>Bridge</b> in the <b>Mode</b> field, select either <b>PPPoA</b> or <b>RFC 1483</b> . If you select <b>Routing</b> in the <b>Mode</b> field, select <b>PPPoA</b> , <b>RFC 1483</b> , <b>ENET ENCAP</b> or <b>PPPoE</b> .
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are <b>VC</b> or <b>LLC</b> .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select <b>UBR</b> (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select <b>VBR</b> (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	(PPPoE only) Type the name of your PPPoE service here.
User Name	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.
IP Address	This option is available if you select <b>Routing</b> in the <b>Mode</b> field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the <b>IP Address</b> field below.
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.

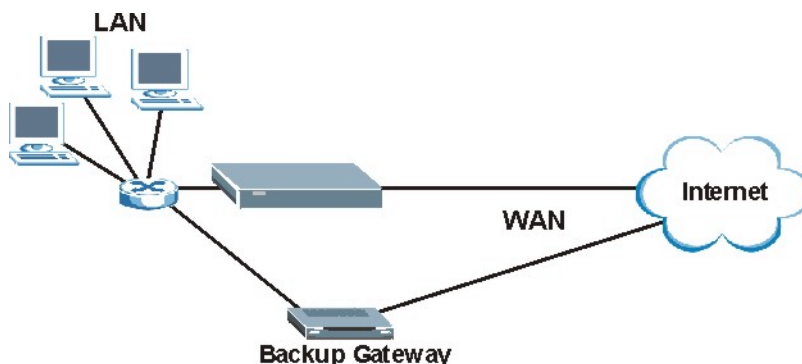
**Table 12** WAN Setup (continued)

LABEL	DESCRIPTION
Max Idle Timeout	Specify an idle time-out in the <b>Max Idle Timeout</b> field when you select <b>Connect on Demand</b> . The default setting is 0, which means the Internet session will not timeout.
PPPoE Passthrough (PPPoE encapsulation only)	<p>This field is available when you select <b>PPPoE</b> encapsulation.</p> <p>In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address.</p> <p>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.</p>
Subnet Mask (ENET ENCAP encapsulation only)	<p>Enter a subnet mask in dotted decimal notation.</p> <p>Refer to <a href="#">Appendix C on page 144</a> in the to calculate a subnet mask If you are implementing subnetting.</p>
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select <b>ENET ENCAP</b> in the <b>Encapsulation</b> field
Zero Configuration	<p>This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode.</p> <p>Select <b>Yes</b> to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes.</p> <p>Select <b>No</b> to disable this feature. You must manually configure the ZyXEL Device for Internet access.</p>
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 6.7 Traffic Redirect

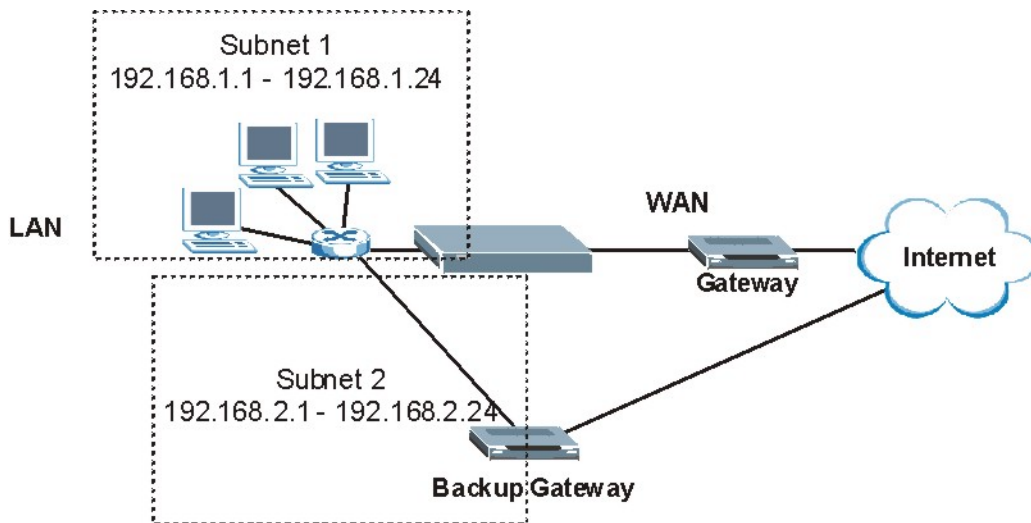
Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet. An example is shown in the figure below.

**Figure 20** Traffic Redirect Example



The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the ZyXEL Device itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

**Figure 21** Traffic Redirect LAN Setup



## 6.8 Configuring WAN Backup

To change your ZyXEL Device's WAN backup settings, click **WAN**, then **WAN Backup**. The screen appears as shown.

**Figure 22** WAN Backup

The following table describes the labels in this screen.

**Table 13** WAN Backup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select <b>DSL Link</b> to have the ZyXEL Device check if the connection to the DSLAM is up. Select <b>ICMP</b> to have the ZyXEL Device periodically ping the IP addresses configured in the <b>Check WAN IP Address</b> fields.
Check WAN IP Address1-3	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address).  <b>Note:</b> If you activate either traffic redirect or dial backup, you must configure at least one IP address here.  When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the <b>Check WAN IP Address</b> field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection.  Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.

**Table 13** WAN Backup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the <b>Check WAN IP Address</b> field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	
Active	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down.  <b>Note:</b> If you activate traffic redirect, you must configure at least one <b>Check WAN IP Address</b> .
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.





# CHAPTER 7

## Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the ZyXEL Device.

### 7.1 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 to a different IP address known within another network.

#### 7.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 14** NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

**Note:** NAT never changes the IP address (either local or global) of an **outside** host.

## 7.1.2 What NAT Does

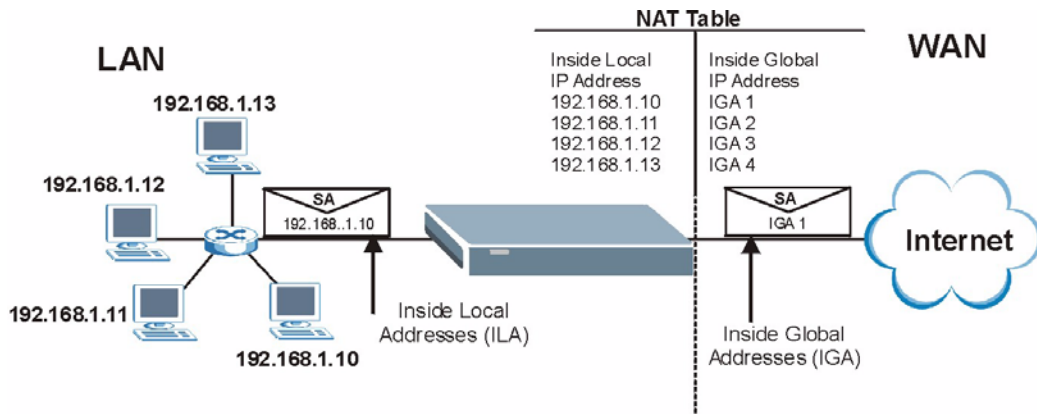
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 15 on page 69](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

## 7.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

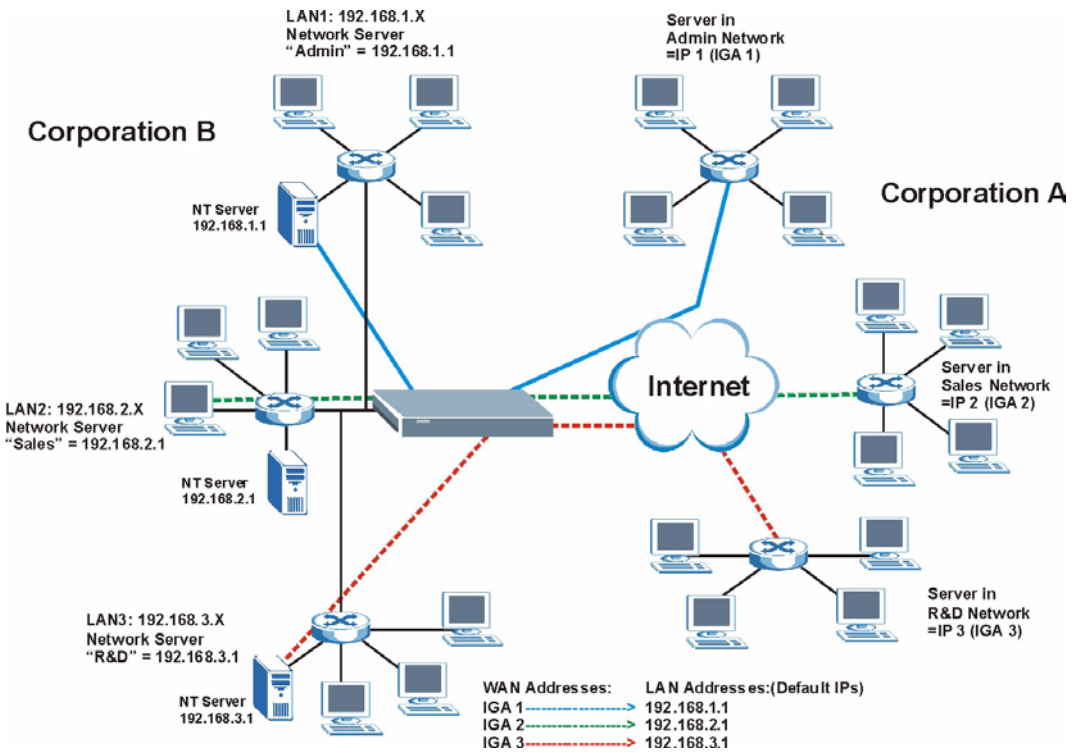
Figure 23 How NAT Works



### 7.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyXEL Device can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 24 NAT Application With IP Alias



### 7.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload:** In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

**Note:** Port numbers do **not** change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

**Table 15** NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1 ↔ IGA1
Many-to-One (SUA/PAT)	ILA1 ↔ IGA1 ILA2 ↔ IGA1 ...
Many-to-Many Overload	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA1 ILA4 ↔ IGA2 ...
Many-to-Many No Overload	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA3 ...
Server	Server 1 IP ↔ IGA1 Server 2 IP ↔ IGA1 Server 3 IP ↔ IGA1

## 7.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 15 on page 69](#).

- Note:** 1. Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.
2. Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

## 7.3 SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

### 7.3.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

**Note:** If you do not assign an IP address in **Server Set 1** (default server) the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

### 7.3.2 Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

**Table 16** Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79

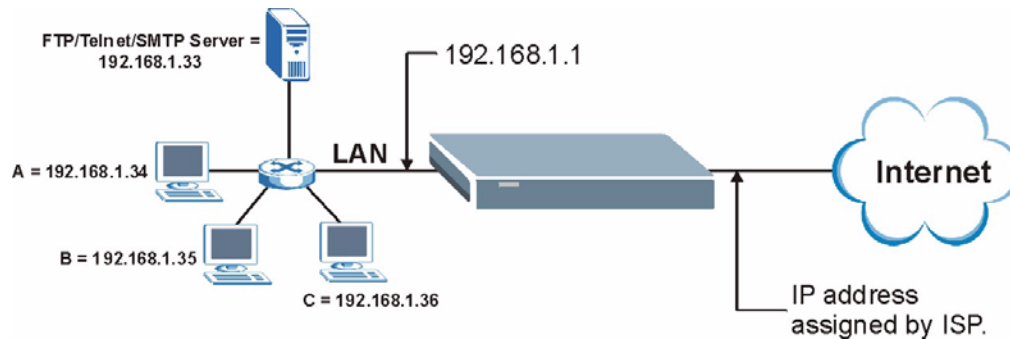
**Table 16** Services and Port Numbers (continued)

SERVICES	PORT NUMBER
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

### 7.3.3 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

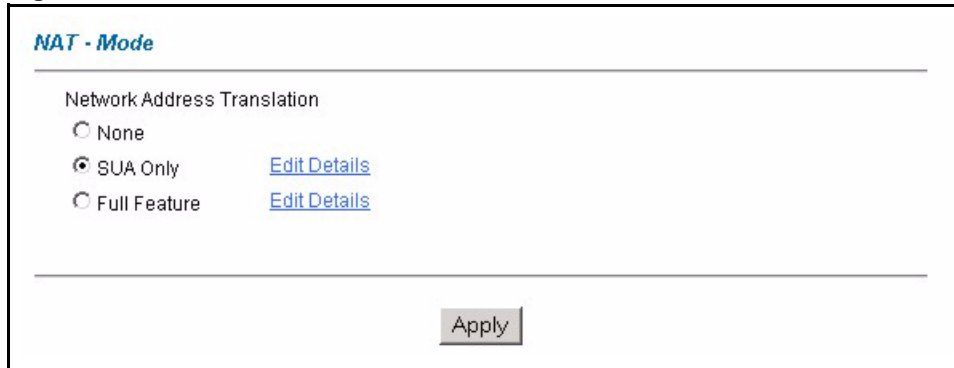
IP address assigned by ISP.

**Figure 25** Multiple Servers Behind NAT Example

## 7.4 Selecting the NAT Mode

Click **NAT** to open the following screen.

**Figure 26** NAT Mode



The following table describes the labels in this screen.

**Table 17** NAT Mode

LABEL	DESCRIPTION
None	Select this radio button to disable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device. The ZyXEL Device uses Address Mapping Set 1 in the <b>NAT - Edit SUA/NAT Server Set</b> screen.
Edit Details	Click this link to go to the <b>NAT - Edit SUA/NAT Server Set</b> screen.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Edit Details	Click this link to go to the <b>NAT - Address Mapping Rules</b> screen.
Apply	Click <b>Apply</b> to save your configuration.

## 7.5 Configuring SUA Server

**Note:** If you do not assign an IP address in **Server Set 1** (default server), the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Click **NAT**, select **SUA Only** and click **Edit Details** to open the following screen.

Refer to [Table 16 on page 70](#) for port numbers commonly used for particular services.



**Figure 27** Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

The following table describes the labels in this screen.

**Table 18** Edit SUA/NAT Server Set

LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the <b>End Port No.</b> field. To forward a series of ports, enter the start port number here and the end port number in the <b>End Port No.</b> field.
End Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the <b>Start Port No.</b> field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the <b>Start Port No.</b> field above.
IP Address	Enter your server IP address in this field.
Save	Click <b>Save</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previous configuration.

## 7.6 Configuring Address Mapping

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your ZyXEL Device's address mapping settings, click **NAT**, Select **Full Feature** and click **Edit Details** to open the following screen.

**Figure 28** Address Mapping Rules

	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
<a href="#">Rule 1</a>	...	...	...	...	-
<a href="#">Rule 2</a>	...	...	...	...	-
<a href="#">Rule 3</a>	...	...	...	...	-
<a href="#">Rule 4</a>	...	...	...	...	-
<a href="#">Rule 5</a>	...	...	...	...	-
<a href="#">Rule 6</a>	...	...	...	...	-
<a href="#">Rule 7</a>	...	...	...	...	-
<a href="#">Rule 8</a>	...	...	...	...	-
<a href="#">Rule 9</a>	...	...	...	...	-
<a href="#">Rule 10</a>	...	...	...	...	-

Back

The following table describes the labels in this screen.

**Table 19** Address Mapping Rules

LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-one</b> and <b>Server</b> mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for <b>Many-to-One</b> and <b>Server</b> mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is <b>N/A</b> for <b>One-to-one</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.

**Table 19** Address Mapping Rules (continued)

LABEL	DESCRIPTION
Type	<p><b>1-1:</b> One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p><b>M-1:</b> Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p><b>M-M Ov (Overload):</b> Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p><b>MM No (No Overload):</b> Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p><b>Server:</b> This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Back	Click <b>Back</b> to return to the <b>NAT Mode</b> screen.

## 7.7 Editing an Address Mapping Rule

To edit an address mapping rule, click the rule's link in the **NAT Address Mapping Rules** screen to display the screen shown next.

**Figure 29** Address Mapping Rule Edit

**NAT - Edit Address Mapping Rule 1**

Type: One-to-One

Local Start IP: 0.0.0.0

Local End IP: N/A

Global Start IP: 0.0.0.0

Global End IP: N/A

Server Mapping Set: N/A [Edit Details](#)

Apply Cancel Delete

The following table describes the labels in this screen.

**Table 20** Address Mapping Rule Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <ul style="list-style-type: none"> <li>• <b>One-to-One:</b> One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.</li> <li>• <b>Many-to-One:</b> Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</li> <li>• <b>Many-to-Many Overload:</b> Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</li> <li>• <b>Many-to-Many No Overload:</b> Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</li> <li>• <b>Server:</b> This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</li> </ul>
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Server Mapping Set	Only available when <b>Type</b> is set to <b>Server</b> . Select a number from the drop-down menu to choose a server set from the <b>NAT - Address Mapping Rules</b> screen.
Edit Details	Click this link to go to the <b>NAT - Edit SUA/NAT Server Set</b> screen to edit a server set that you have selected in the <b>Server Mapping Set</b> field.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.
Delete	Click <b>Delete</b> to exit this screen without saving.



# CHAPTER 8

## Dynamic DNS Setup

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

### 8.1 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with [www.dyndns.org](http://www.dyndns.org). This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

#### 8.1.1 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](http://www.yourhost.dyndns.org) and still reach your hostname.

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

### 8.2 Configuring Dynamic DNS

To change your ZyXEL Device's DDNS, click **Dynamic DNS**. The screen appears as shown.

**Figure 30** Dynamic DNS

The following table describes the labels in this screen.

**Table 21** Dynamic DNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Host Names	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
User	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# CHAPTER 9

## Time and Date

This screen is not available on all models. Use this screen to configure the ZyXEL Device's time and date settings.

### 9.1 Configuring Time and Date

To change your ZyXEL Device's time and date, click **Time And Date**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

**Figure 31** Time and Date

*Time and Date*

---

**Time Server**

Use Protocol when Bootup None

IP Address or URL N/A

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

Daylight Savings

Start Date 1 month 1 day

End Date 1 month 1 day

Synchronize system clock with Time Server now.  
(This may take up to 60 seconds.)

**Date**

Current Date 2000 - 01 - 01

New Date (yyy-mm-dd) 2000 - 01 - 01

**Time**

Current Time 01 : 10 : 51

New Time 01 : 10 : 51

---

Apply
Cancel



The following table describes the labels in this screen.

**Table 22** Time and Date

LABEL	DESCRIPTION
Time Server	
Use Protocol when Bootup	<p>Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.</p> <p>The main difference between them is the format.</p> <p><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.</p> <p><b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p><b>NTP (RFC 1305)</b> is similar to <b>Time (RFC 868)</b>.</p> <p>Select <b>None</b> to enter the time and date manually.</p>
IP Address or URL	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time and Date	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected <b>Daylight Savings</b> .
End Date	Enter the month and day that your daylight-savings time ends on if you selected <b>Daylight Savings</b> .
Synchronize system clock with Time Server now.	<p>Select this option to have your ZyXEL Device use the time server (that you configured above) to set its internal system clock.</p> <p>Please wait for up to 60 seconds while the ZyXEL Device locates the time server. If the ZyXEL Device cannot find the time server, please check the time server protocol and its IP address. If the IP address was entered correctly, try pinging it for example to test the connection.</p>
Date	
Current Date	<p>This field displays the date of your ZyXEL Device.</p> <p>Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.</p>
New Date (yyyy-mm-dd)	<p>This field displays the last updated date from the time server.</p> <p>When you select <b>None</b> in the <b>Use Protocol when Bootup</b> field, enter the new date in this field and then click <b>Apply</b>.</p>
Time	
Current Time	<p>This field displays the time of your ZyXEL Device.</p> <p>Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.</p>
New Time	<p>This field displays the last updated time from the time server.</p> <p>When you select <b>None</b> in the <b>Use Protocol when Bootup</b> field, enter the new time in this field and then click <b>Apply</b>.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# CHAPTER 10

## Remote Management Configuration

This chapter provides information on configuring remote management.

### 10.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

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

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

- 1 Telnet
- 2 HTTP

#### 10.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

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

## 10.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

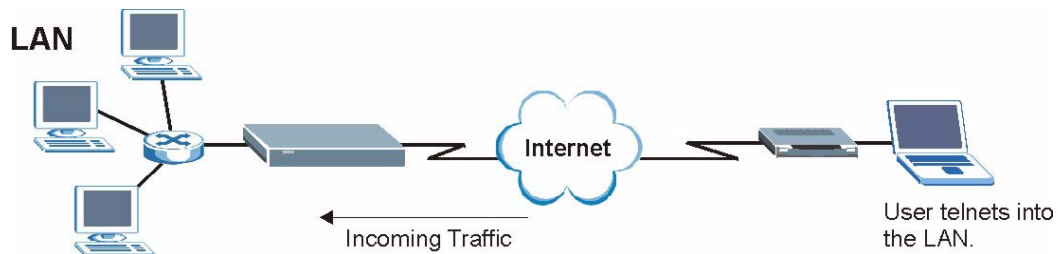
## 10.1.3 System Timeout

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

## 10.2 Telnet

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

**Figure 32** Telnet Configuration on a TCP/IP Network



## 10.3 FTP

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

## 10.4 Web

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

## 10.5 Configuring Remote Management

Click **Remote Management** to open the following screen.

**Figure 33** Remote Management

*Remote Management Control*

---

Server Type	Access Status	Port	Secured Client IP
<b>Telnet</b>	All <input type="button" value="v"/>	23	0.0.0.0
<b>FTP</b>	All <input type="button" value="v"/>	21	0.0.0.0
<b>Web</b>	All <input type="button" value="v"/>	80	0.0.0.0

---

The following table describes the labels in this screen.

**Table 23** Remote Management

LABEL	DESCRIPTION
Server Type	Each of these labels denotes a service that you may use to remotely manage the ZyXEL Device.
Access Status	Select the access interface. Choices are <b>All</b> , <b>LAN Only</b> , <b>WAN Only</b> and <b>Disable</b> .
Port	This field shows the port number for the remote management service. You may change the port number for a service in this field, but you must use the same port number to use that service for remote management.
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyXEL Device. Type an IP address to restrict access to a client with a matching IP address.
Apply	Click <b>Apply</b> to save your settings back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 11

## Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

### 11.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See [Section 11.2.1 on page 87](#) for configuration instructions.

#### 11.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

#### 11.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

### 11.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## 11.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See the following sections for examples of installing and using UPnP.

### 11.2.1 Configuring UPnP

From the **Site Map** in the main menu, click **UPnP** under **Advanced Setup** to display the screen shown next.

**Figure 34** Configuring UPnP

UPNP

Enable the Universal Plug and Play(UPnP) Service

Allow users to make configuration changes through UPnP

Apply Cancel

The following table describes the labels in this screen.

**Table 24** Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click <b>Apply</b> to save the setting to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 11.3 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

### Installing UPnP in Windows Me

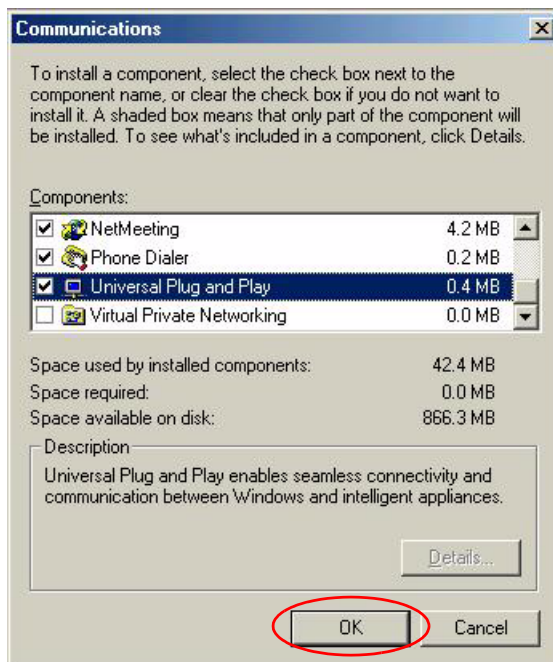
Follow the steps below to install the UPnP in Windows Me.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



**Figure 35** Add/Remove Programs: Windows Setup: Communication

- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

**Figure 36** Add/Remove Programs: Windows Setup: Communication: Components

- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

## Installing UPnP in Windows XP

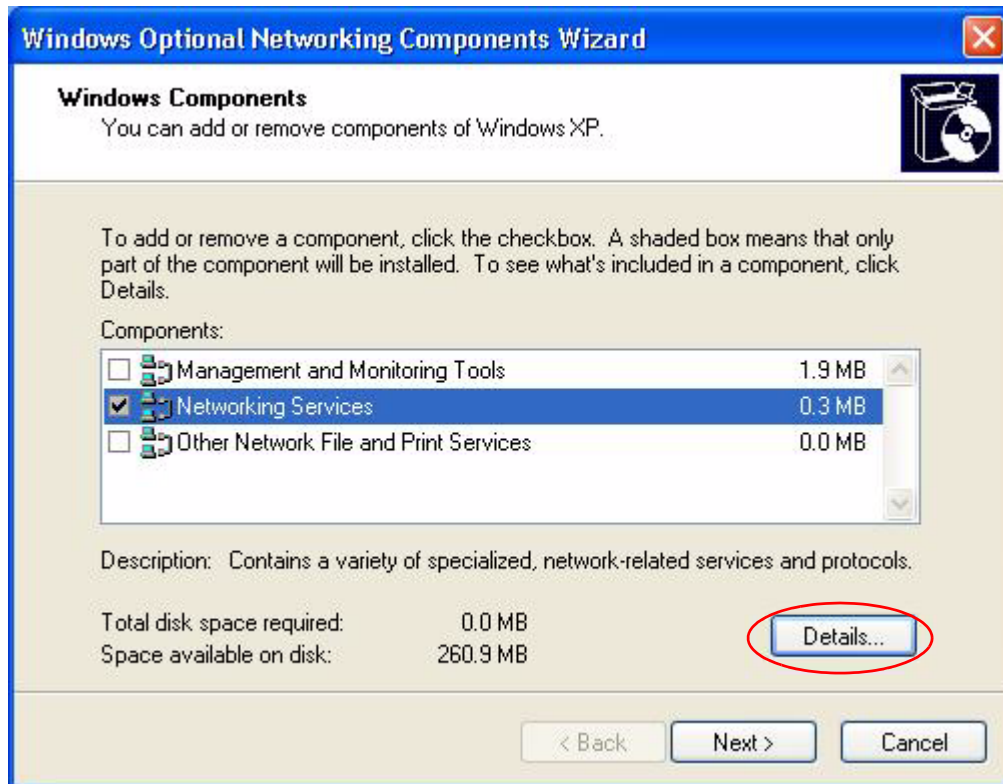
Follow the steps below to install the UPnP in Windows XP.

- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ....**

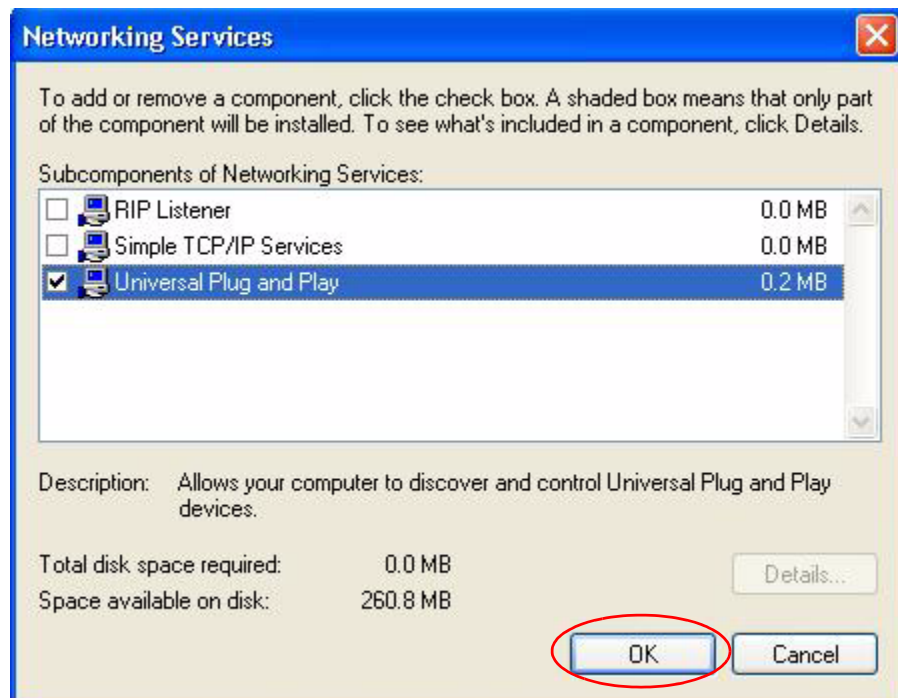
**Figure 37** Network Connections



- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 38** Windows Optional Networking Components Wizard

**5** In the **Networking Services** window, select the **Universal Plug and Play** check box.

**Figure 39** Networking Services

- Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

## 11.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

### Auto-discover Your UPnP-enabled Network Device

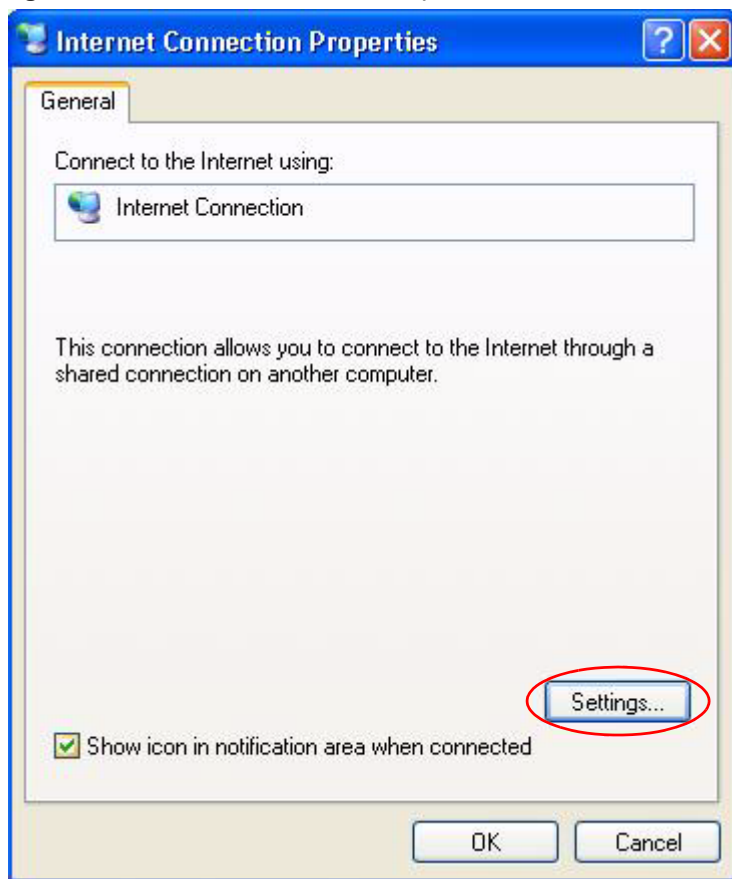
- Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- Right-click the icon and select **Properties**.

**Figure 40** Network Connections

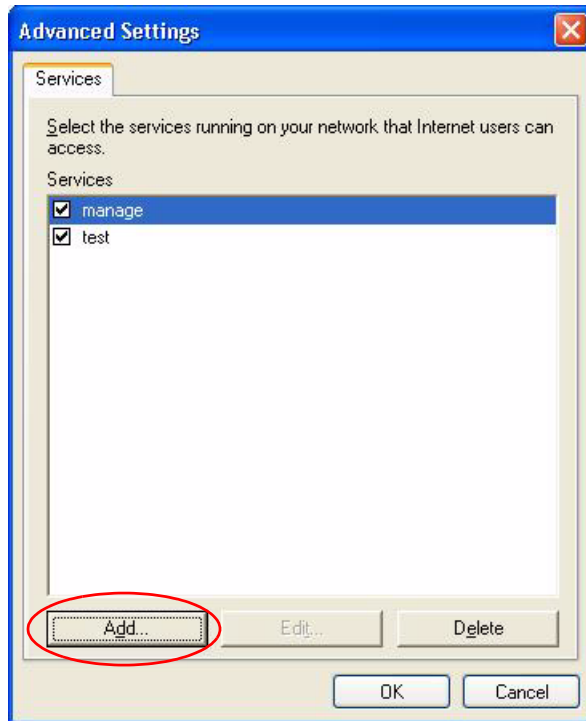


- In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

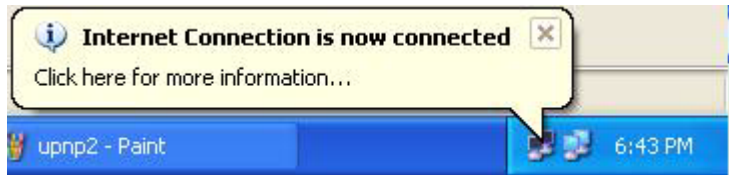
**Figure 41** Internet Connection Properties



- 4** You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 42** Internet Connection Properties: Advanced Settings**Figure 43** Internet Connection Properties: Advanced Settings: Add

- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.
- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

**Figure 44** System Tray Icon

- 7 Double-click on the icon to display your current Internet connection status.

**Figure 45** Internet Connection Status

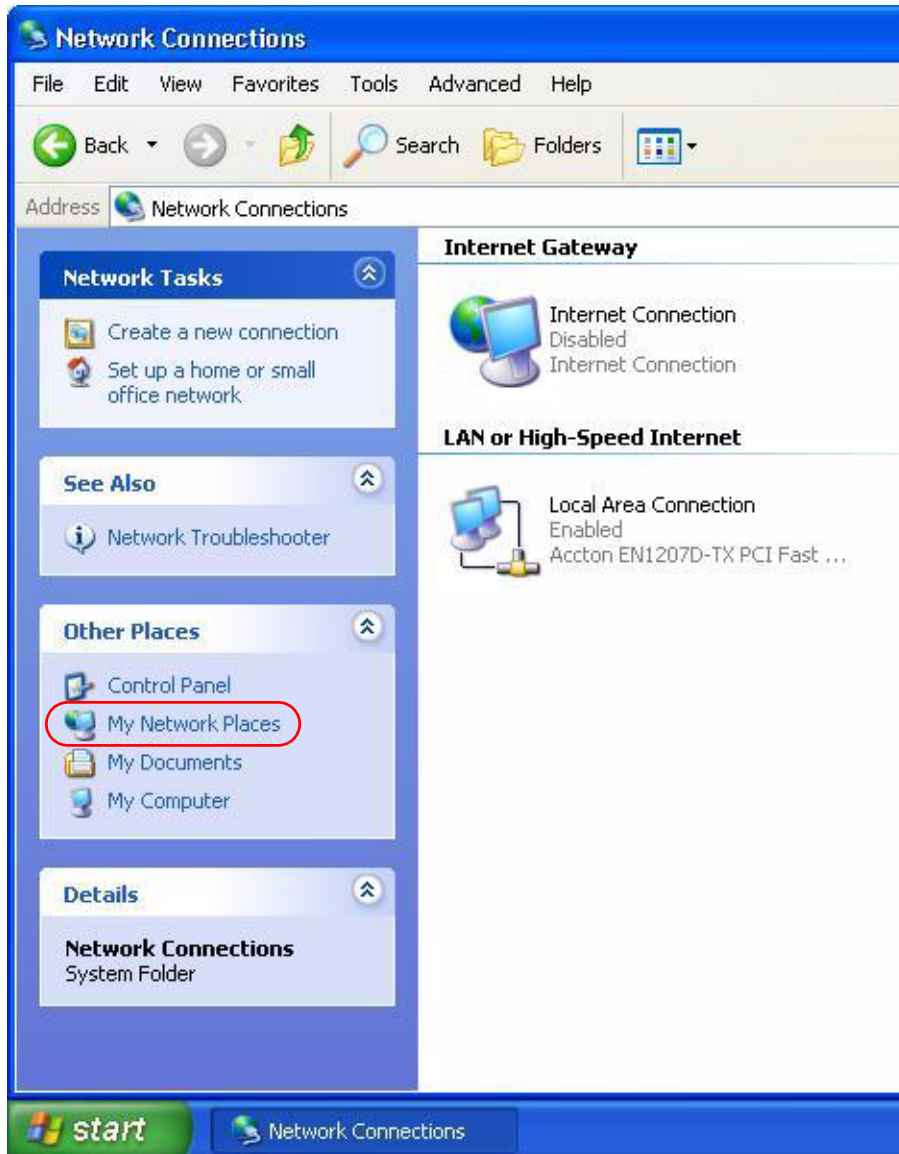
### Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.

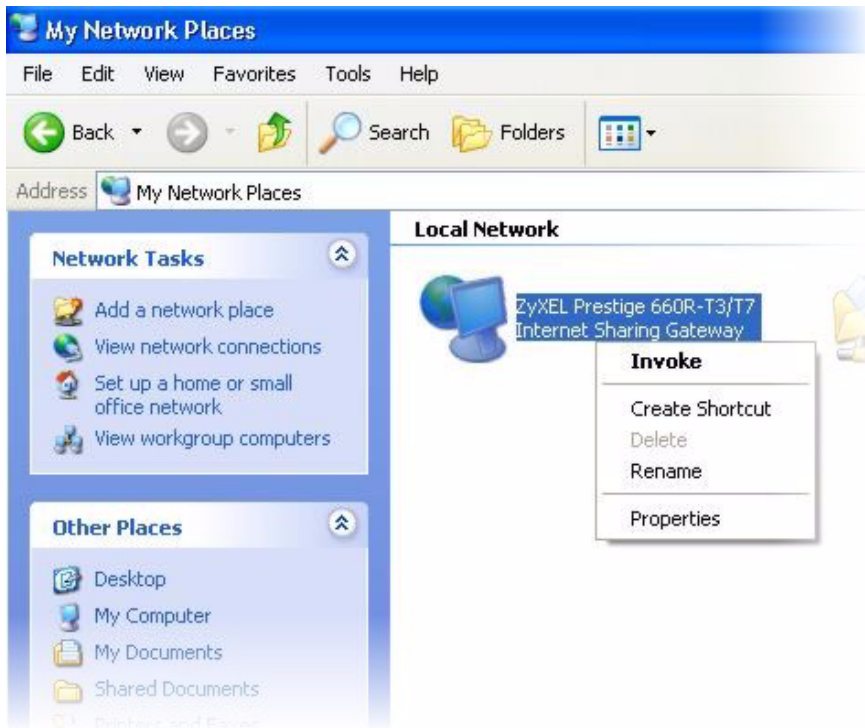
Figure 46 Network Connections



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.



**Figure 47** Network Connections: My Network Places



- 6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

**Figure 48** Network Connections: My Network Places: Properties: Example



# CHAPTER 12

## Maintenance

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

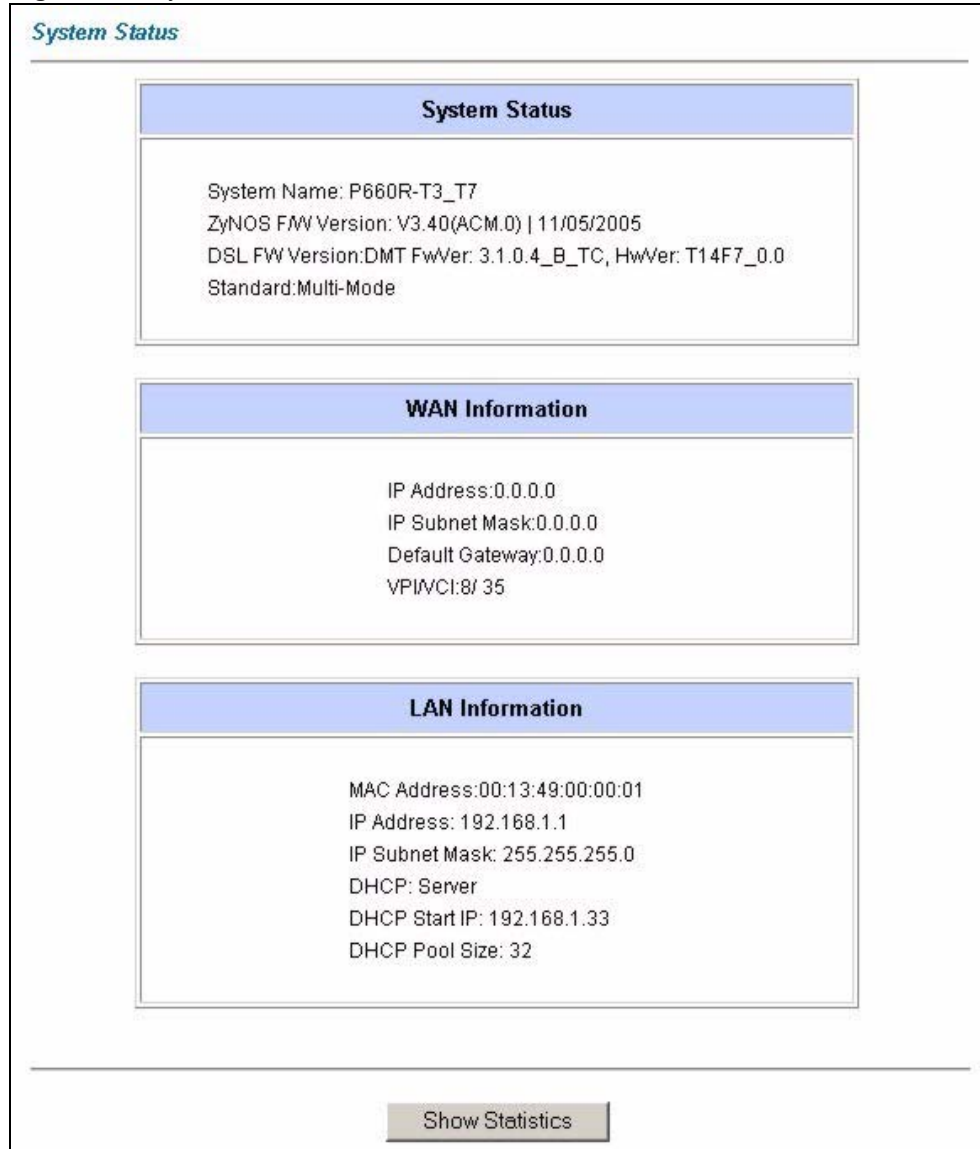
### 12.1 Maintenance Overview

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

### 12.2 System Status Screen

Click **System Status** to open the following screen. You can use this screen to monitor your ZyXEL Device. Note that these fields are READ-ONLY and only for diagnostic purposes.

**Figure 49** System Status



The following table describes the fields in this screen.

**Table 25** System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your ZyXEL Device. It is for identification purposes.
ZyNOS Firmware Version	This is the ZyNOS firmware version and the date the firmware was created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL FW Version	This is the DSL firmware version associated with your ZyXEL Device.
Standard	This is the standard that your ZyXEL Device is using.
WAN Information	
IP Address	This is the WAN port IP address.

**Table 25** System Status (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZYXEL Device.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - <b>Server, Relay</b> (not all Zyxel Device models) or <b>None</b> .
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
Show Statistics	Click <b>Show Statistics</b> to see the performance statistics such as number of packets sent and number of packets received for each port.

## 12.2.1 System Statistics

Click **Show Statistics** in the **System Status** screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

**Figure 50** System Status: Show Statistics

**System up Time: 0:36:42**  
CPU Load: **13.04%**

**WAN Port Statistics:**  
Link Status: **Down**  
Upstream Speed: **0 kbps**  
Downstream Speed: **0 kbps**

Node-Link	Status	TxPkts	RxPkts	Errors	Tx B/s	Rx B/s	Up Time
1-ENET	N/A	0	0	0	0	0	0:00:00

LAN Port Statistics:

Interface:	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full Duplex	2184	1867	0

Poll Interval(s) :

The following table describes the labels in this screen.

**Table 26** System Status: Show Statistics

LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.
CPU Load	This field specifies the percentage of CPU utilization.
LAN or WAN Port Statistics	This is the WAN or LAN port.
Link Status	This is the status of your WAN link.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Interface	This field displays the type of port.
Status	For the WAN port, this displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation. For a LAN port, this shows the port speed and duplex setting.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval</b> field above.
Stop	Click this button to halt the refreshing of the system statistics.

## 12.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Maintenance**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

**Figure 51** DHCP Table

Host Name	IP Address	MAC Address
tw	192.168.1.33	00-00-E8-7C-14-80

The following table describes the fields in this screen.

**Table 27** DHCP Table

LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the <b>Host Name</b> field.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed host name. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

## 12.4 Any IP Table Screen

Click **Maintenance, Any IP**. The Any IP table shows current read-only information (including the IP address and the MAC address) of all network devices that use the Any IP feature to communicate with the ZyXEL Device. Refer to [Section 5.5 on page 51](#) for more information.

**Figure 52** Any IP Table

#	IP Address	MAC Address
1	192.168.10.1	00:50:ba:ad:4f:81

Refresh

The following table describes the labels in this screen.

**Table 28** Any IP Table

LABEL	DESCRIPTION
#	This field displays the index number.
IP Address	This field displays the IP address of the network device.

**Table 28** Any IP Table

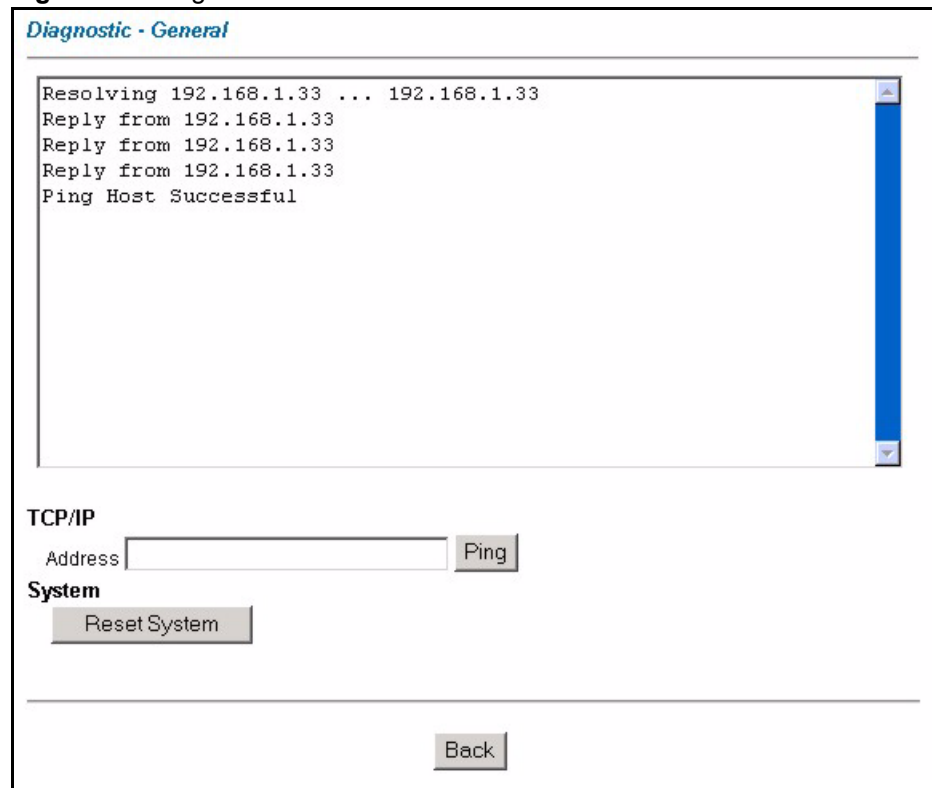
LABEL	DESCRIPTION
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed IP address. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click <b>Refresh</b> to update this screen.

## 12.5 Diagnostic Screens

These read-only screens display information to help you identify problems with the ZyXEL Device.

### 12.5.1 Diagnostic General Screen

Click **Diagnostic** and then **General** to open the screen shown next.

**Figure 53** Diagnostic: General

The following table describes the labels in this screen.

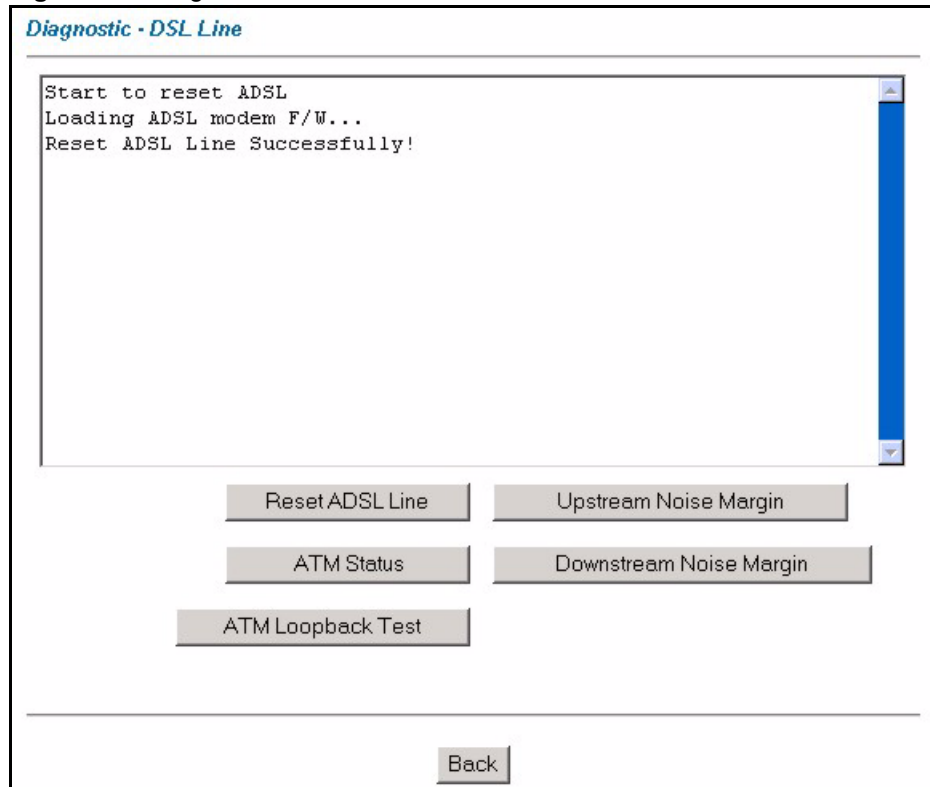
**Table 29** Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the ZyXEL Device. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click <b>OK</b> to proceed.
Back	Click this button to go back to the main <b>Diagnostic</b> screen.

## 12.5.2 Diagnostic DSL Line Screen

Click **Diagnostic** and then **DSL Line** to open the screen shown next.

**Figure 54** Diagnostic: DSL Line





The following table describes the labels in this screen.

**Table 30** Diagnostic: DSL Line

LABEL	DESCRIPTION
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
Back	Click this button to go back to the main <b>Diagnostic</b> screen.

## 12.6 Firmware Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a .bin extension, for example, "ZyXEL.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

**Note:** Only use firmware for your device's specific model. Refer to the label on the bottom of your device.

Click **Firmware** to open the following screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

**Figure 55** Firmware Upgrade

**FIRMWARE**

---

**Firmware Upgrade**

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click **UPLOAD**.

File Path:  **Browse...** **Upload**

---

**CONFIGURATION FILE**

Click **Reset** to clear all user-defined configurations and return to the factory defaults.

**Reset**

The following table describes the labels in this screen.

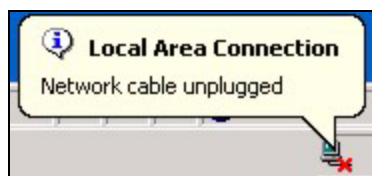
**Table 31** Firmware Upgrade

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.
Reset	Click this button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. Refer to <a href="#">Section 2.2 on page 31</a> .

**Note:** Do not turn off the ZyXEL Device while firmware upload is in progress!

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

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

**Figure 56** Network Temporarily Disconnected

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

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

**Figure 57** Error Message

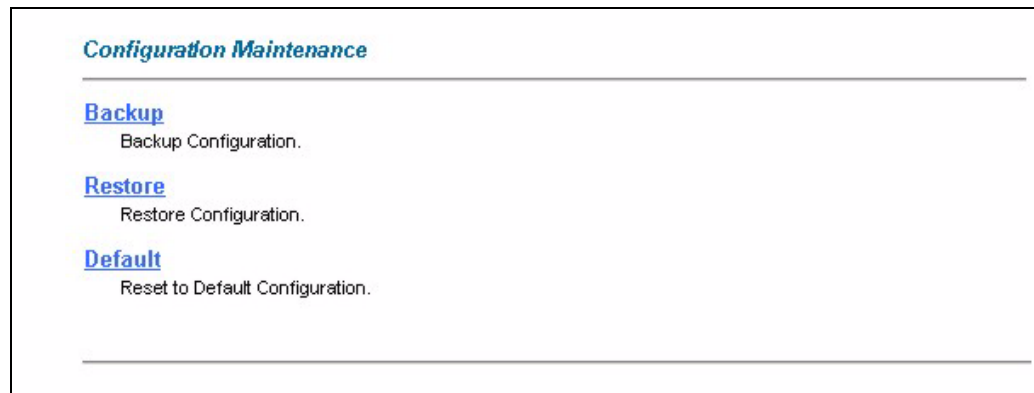


## 12.7 Configuration Screen

Information related to backing up configuration, restoring configuration and resetting configuration to factory defaults appears as shown next. The following screens are not available on all models.

Click **Configuration** to see the following screen. You can choose to backup, restore or reset your configuration.

**Figure 58** Configuration



### 12.7.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL 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.

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

**Figure 59** Backup Configuration

The following table describes the labels in this screen.

**Table 32** Backup Configuration

LABEL	DESCRIPTION
Back	Click this button to go back to the main <b>Configuration</b> menu.
Backup	Click this button to save ZyXEL Device's current configuration to your computer.

## 12.7.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device. Click **Configuration** and then **Restore** to display the screen shown next.

**Figure 60** Restore Configuration

The following table describes the labels in this screen.

**Table 33** Maintenance Restore Configuration

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

**Table 33** Maintenance Restore Configuration

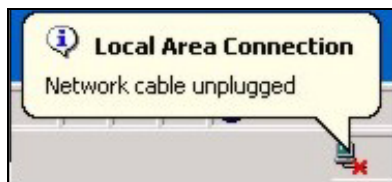
LABEL	DESCRIPTION
Upload	Click <b>Upload</b> to begin the upload process.
Back	Click this button to go back to the main <b>Configuration</b> screen.

**Note:** Do not turn off the ZyXEL Device while configuration file upload is in progress.

After you see a “Restore Configuration Successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

**Figure 61** Restore Configuration Successful

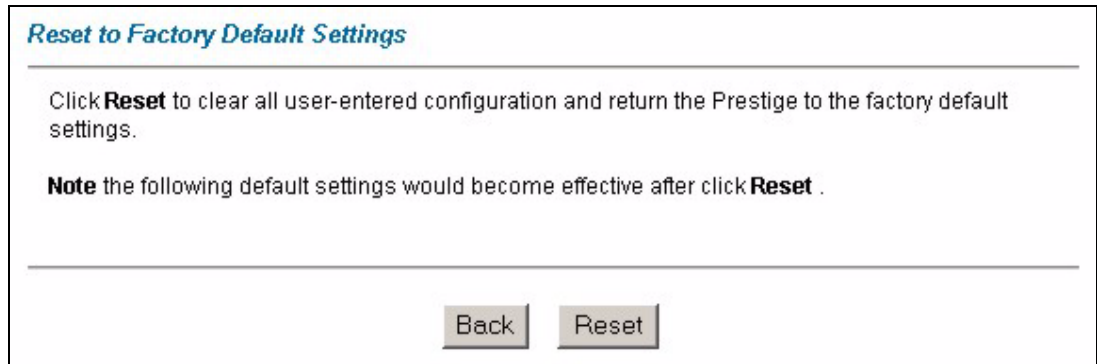
The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 62** Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

### 12.7.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults.

**Figure 63** Reset to Factory Default Settings

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device.



# CHAPTER 13

## Troubleshooting

This chapter covers potential problems and the corresponding remedies.

### 13.1 Problems Starting Up the ZyXEL Device

**Table 34** Troubleshooting the Start-Up of Your ZyXEL Device

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the ZyXEL Device.	<p>Make sure that the ZyXEL Device's power adaptor is connected to the ZyXEL Device and plugged in to an appropriate power source. Check that the ZyXEL Device and the power source are both turned on.</p> <p>Turn the ZyXEL Device off and on.</p> <p>If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</p>

### 13.2 Problems with the LAN LED

**Table 35** Troubleshooting the LAN LED

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections and type (refer to the <i>Quick Start Guide</i> for details).
	Check for faulty Ethernet cables.
	Make sure your computer's Ethernet card is working properly.



## 13.3 Problems with the Password

**Table 36** Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	The default password is "1234". The <b>Password</b> field is case-sensitive. Make sure that you enter the correct password using the proper case. If you have changed the password and have now forgotten it, you will need to upload the default configuration file (Refer to <a href="#">Section 2.2 on page 31</a> in <a href="#">Chapter 2 on page 30</a> ). This restores all of the factory defaults including the password.

## 13.4 Problems with the DSL LED

**Table 37** Troubleshooting the DSL LED

PROBLEM	CORRECTIVE ACTION
The DSL LED is off.	Check the telephone wire and connections between the ZyXEL Device DSL port and the wall jack.
	Make sure that the telephone company has checked your phone line and set it up for DSL service.
	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to <a href="#">Chapter 12 on page 98</a> (web configurator).

## 13.5 Problems with the LAN Interface

**Table 38** Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device from the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to <a href="#">Section 13.2 on page 112</a> . Make sure that the IP address and the subnet mask of the ZyXEL Device and your computer(s) are on the same subnet.
I cannot ping any computer on the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to <a href="#">Section 13.2 on page 112</a> . Make sure that the IP address and the subnet mask of the ZyXEL Device and the computers are on the same subnet.

## 13.6 Problems with the WAN Interface

**Table 39** Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	<p>The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.</p> <p>The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct <b>Service Type</b>, <b>User Name</b> and <b>Password</b> (be sure to use the correct case). Refer to <a href="#">Chapter 6 on page 56</a> (web configurator).</p>

## 13.7 Problems with Internet Access

**Table 40** Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	<p>Make sure the ZyXEL Device is turned on and connected to the network.</p> <p>If the DSL LED is off, refer to <a href="#">Section 13.4 on page 113</a>.</p> <p>Verify your WAN settings. Refer to the chapter on WAN setup (web configurator).</p> <p>Make sure you entered the correct user name and password.</p> <p>If you use PPPoE pass through, make sure that bridge is turned on. See <a href="#">Chapter 14 on page 128</a> for details.</p>
Internet connection disconnects.	<p>If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to <a href="#">Chapter 6 on page 56</a> (web configurator).</p>

## 13.8 Problems with Remote Management

**Table 41** Troubleshooting Remote Management

PROBLEM	CORRECTIVE ACTION
I cannot remotely manage the ZyXEL Device from the LAN or WAN.	Refer to <a href="#">Section 10.1.1 on page 82</a> in <a href="#">Chapter 10 on page 82</a> for scenarios when remote management may not be possible.
	Use the ZyXEL Device's WAN IP address when configuring from the WAN.
	Use the ZyXEL Device's LAN IP address when configuring from the LAN.
	Refer to <a href="#">for instructions on checking your LAN connection</a> .
	Refer to <a href="#">Section 13.5 on page 113</a> for instructions on checking your WAN connection.
	See also <a href="#">Section 13.9 on page 115</a> .

## 13.9 Problems with the Web Configurator

**Table 42** Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTION
I cannot access the web configurator.	Refer to the <i>Quick Start Guide</i> for hardware connections. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details. For WAN access, you must configure remote management to allow server access from the Wan (or all). Refer to the chapters on remote management for details. Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access. If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL. See also <a href="#">Section 13.8 on page 114</a> . See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.
	You may also need to clear your Internet browser's cache. In Internet Explorer, click <b>Tools</b> and then <b>Internet Options</b> to open the <b>Internet Options</b> screen. In the <b>General</b> tab, click <b>Delete Files</b> . In the pop-up window, select the <b>Delete all offline content</b> check box and click <b>OK</b> . Click <b>OK</b> in the <b>Internet Options</b> screen to close it.
	If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address). In Windows, use <b>arp -d</b> at the command prompt to delete all entries in your computer's ARP table.

### 13.9.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

**Note:** Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

#### 13.9.1.1 Internet Explorer Pop-up Blockers

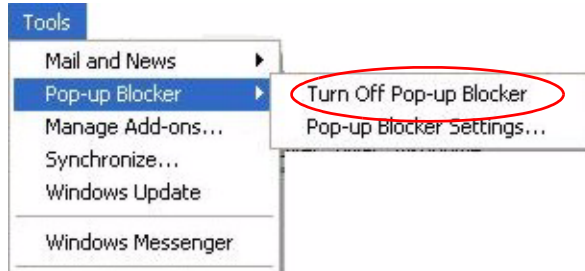
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### 13.9.1.1.1 Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

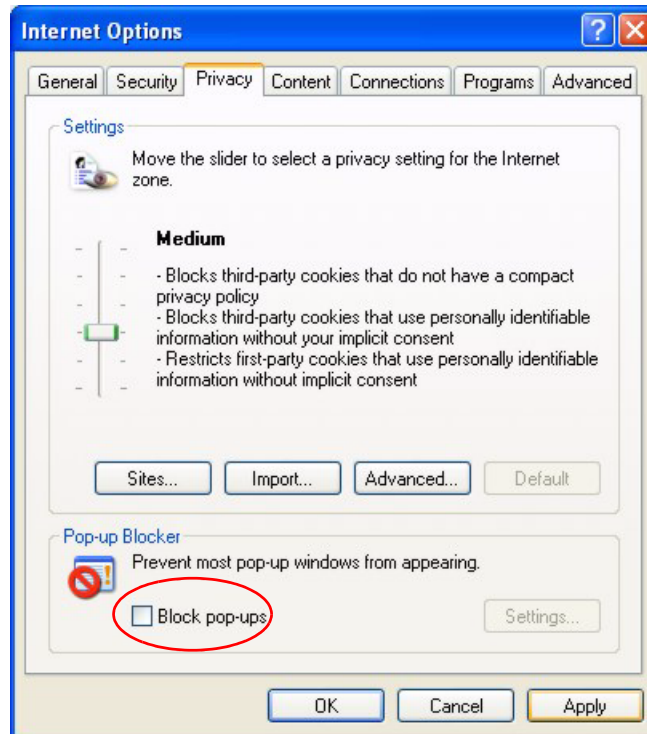
**Figure 64** Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 65** Internet Options



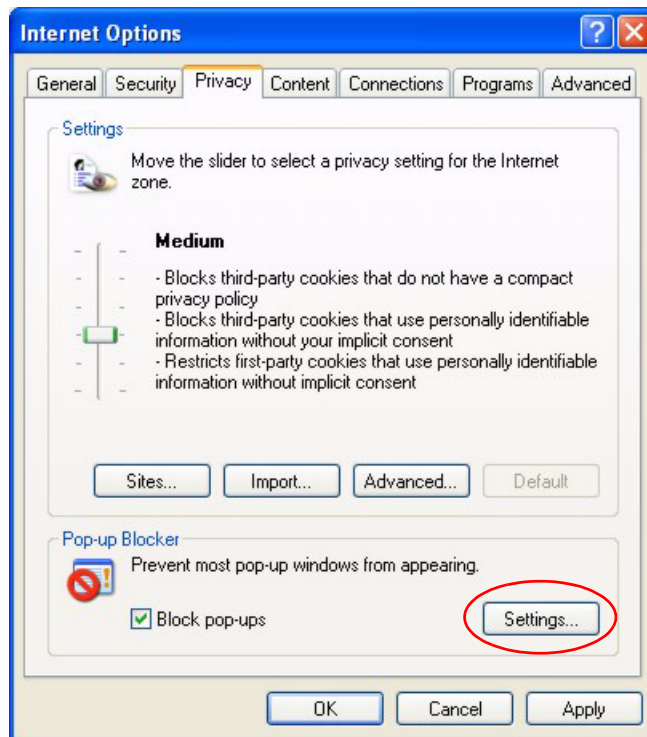
- 3 Click **Apply** to save this setting.

### 13.9.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

**Figure 66** Internet Options



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.
- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 67** Pop-up Blocker Settings

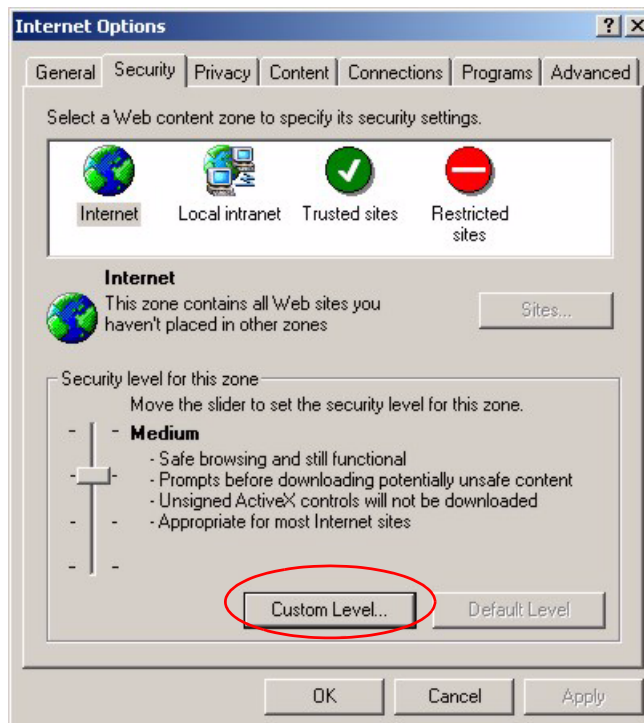
**5** Click **Close** to return to the **Privacy** screen.

**6** Click **Apply** to save this setting.

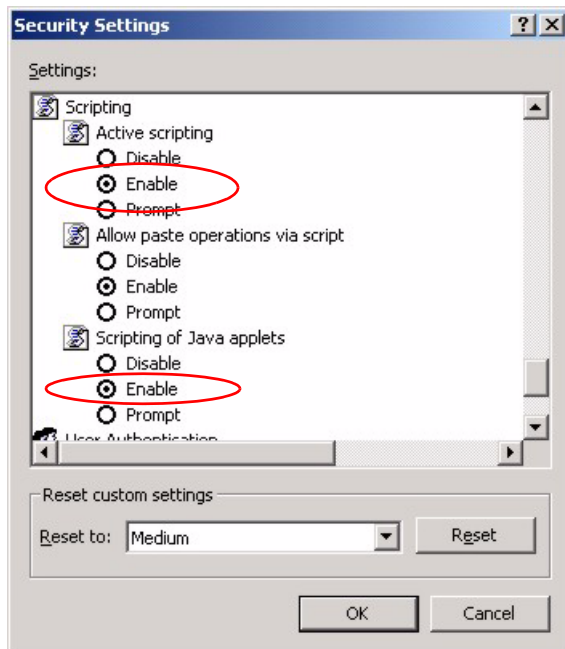
### 13.9.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

**1** In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

**Figure 68** Internet Options

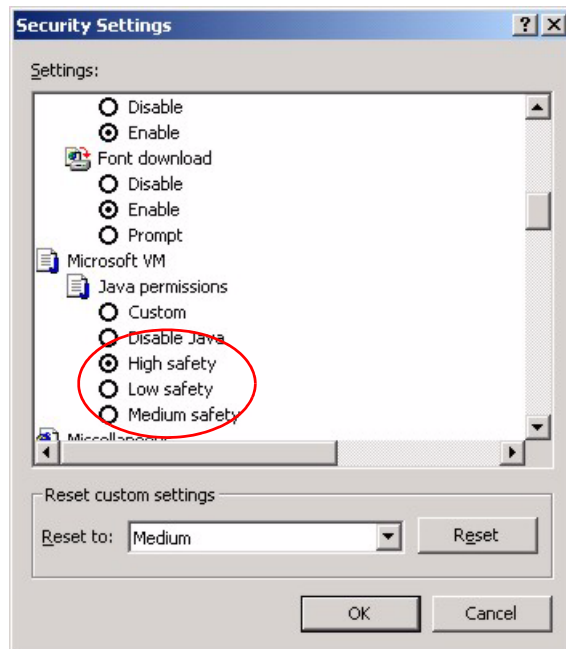
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

**Figure 69** Security Settings - Java Scripting

### 13.9.1.3 Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

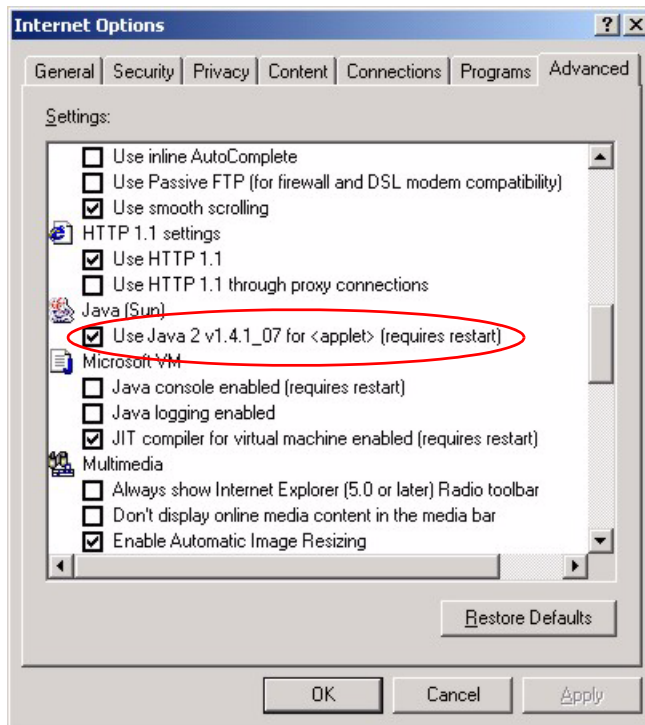


**Figure 70** Security Settings - Java

#### 13.9.1.3.1 JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 71 Java (Sun)





# Appendix A

## Product Specifications

See also the Introduction chapter for a general overview of the key features.

### Specification Tables

**Table 43** Device

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.32 to 192.168.1.64
Dimensions	111 mm(L) × 106.5 mm(W) × 35 mm(H)
Weight	170g
Power Specification	9VAC 1A
Built-in Switch	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Operation Temperature	0° C ~ 40° C
Storage Temperature	-20° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH

**Table 44** Firmware

ADSL Standards	Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G.lite(G.992.2)). ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) RFC 1483 encapsulation over ATM MAC encapsulated routing (ENET encapsulation) VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol. Transparent bridging for unsupported network layer protocols. DHCP Server/Client/Relay RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy UPnP
Management	Embedded Web Configurator CLI (Command Line Interpreter) Remote Management via Telnet or Web SNMP manageable FTP/TFTP for firmware downloading, configuration backup and restoration. Syslog. Built-in Diagnostic Tools for FLASH memory, ADSL circuitry, RAM and LAN port Syslog
NAT/SUA	Port Forwarding 1024 NAT sessions Multimedia application PPTP under NAT/SUA IPSec passthrough SIP ALG passthrough

**Table 44** Firmware (continued)

Static Routes	16 IP and 4 Bridge
Other Features	Any IP Zero Configuration (VC auto-hunting) Traffic Redirect Dynamic DNS IP Alias IP Policy Routing



# 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.

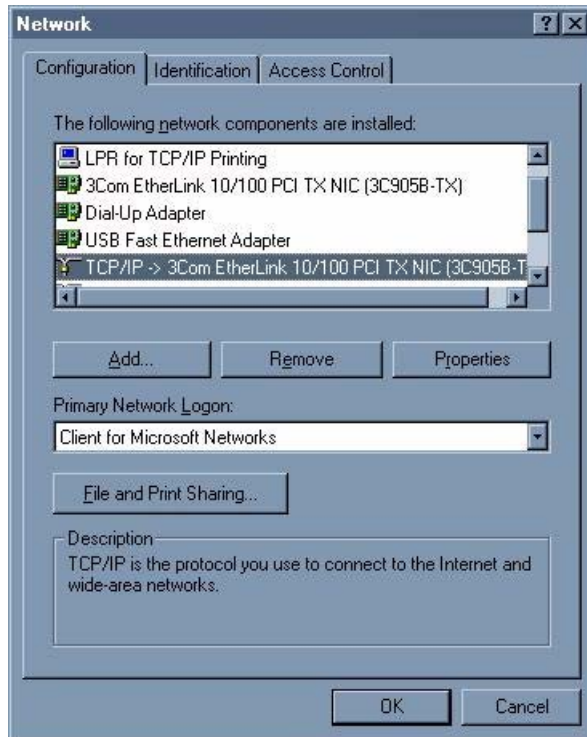
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 ZyXEL Device's LAN port.

### Windows 95/98/Me

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



**Figure 72** 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:

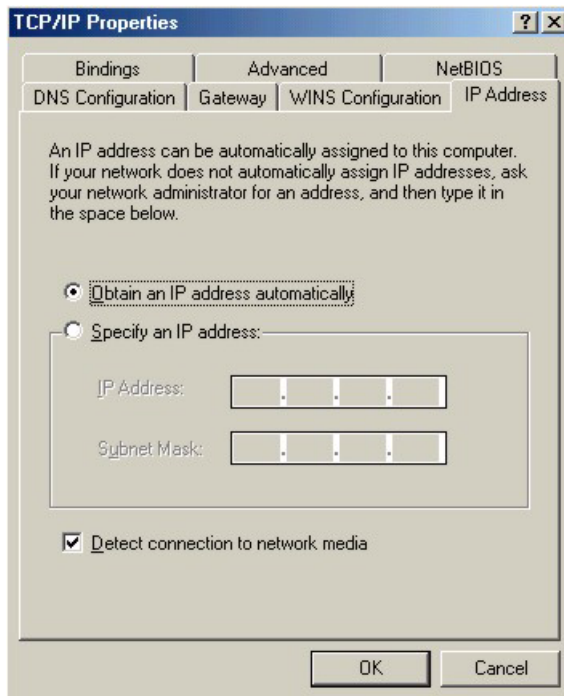
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

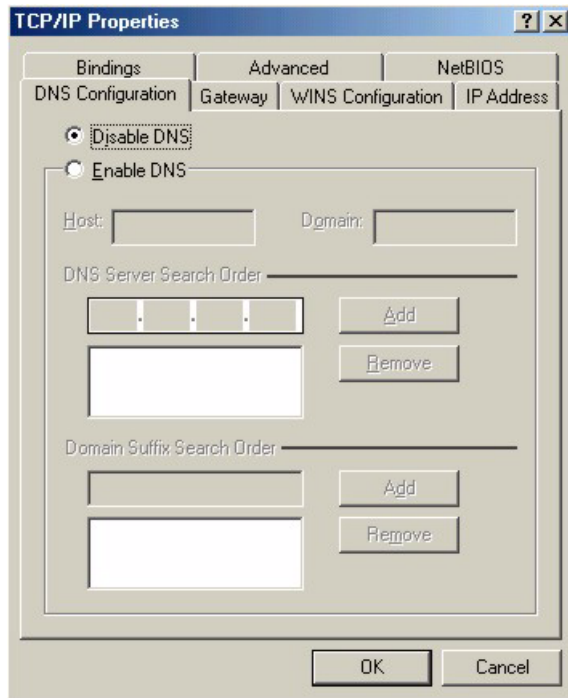
## Configuring

- 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 73** 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).

**Figure 74** 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 ZyXEL Device and restart your computer when prompted.

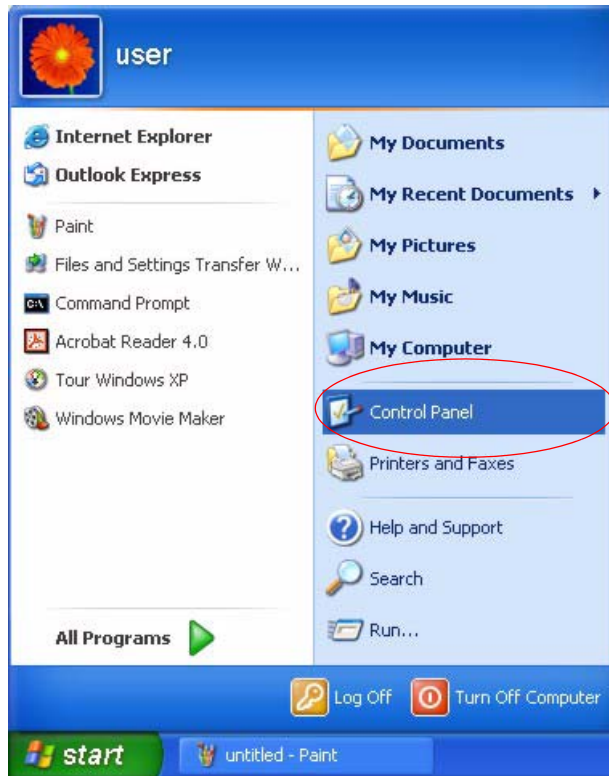
## Verifying Settings

**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.

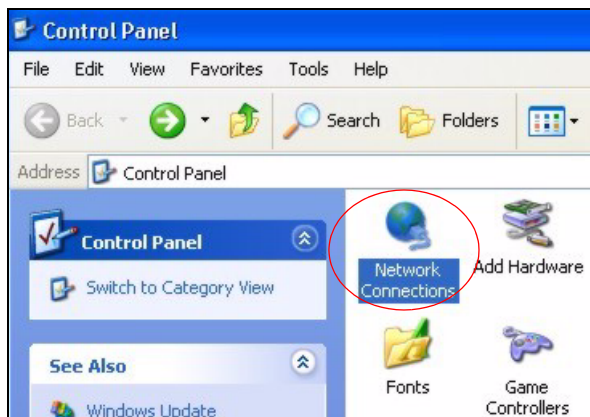
## Windows 2000/NT/XP

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

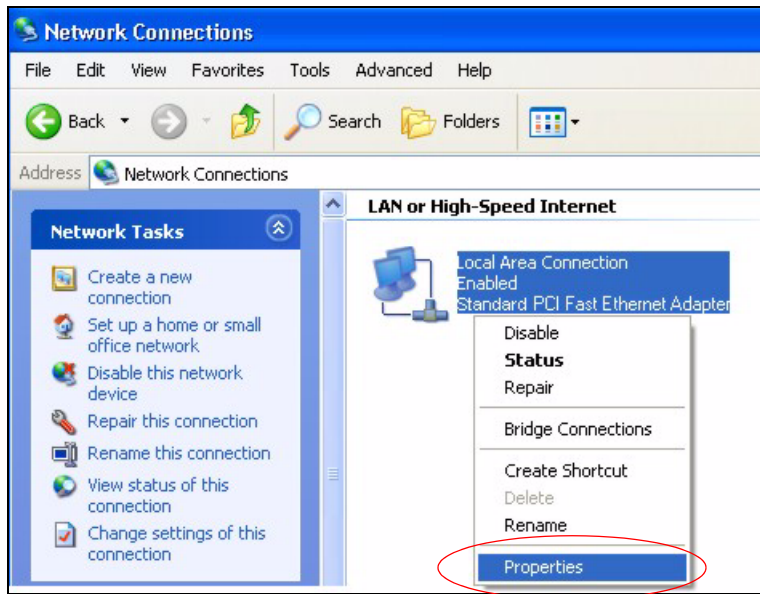
**1** Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 75** Windows XP: Start Menu

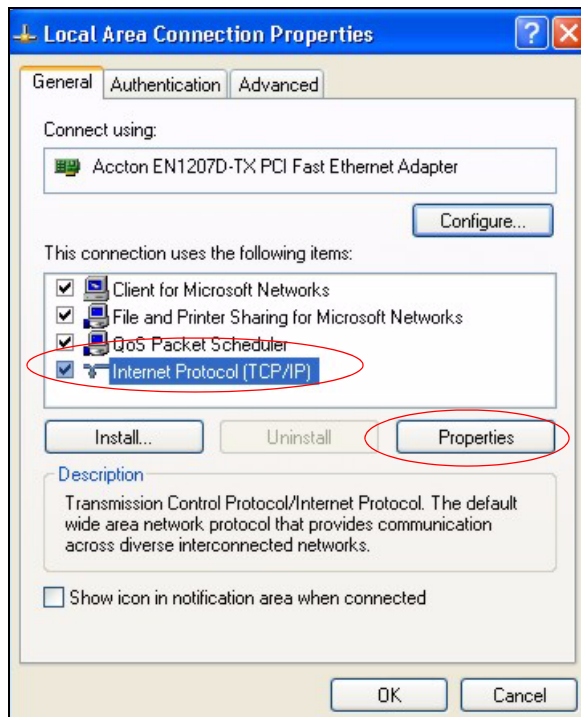
**2** In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

**Figure 76** Windows XP: Control Panel

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

**Figure 77** Windows XP: Control Panel: Network Connections: Properties

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

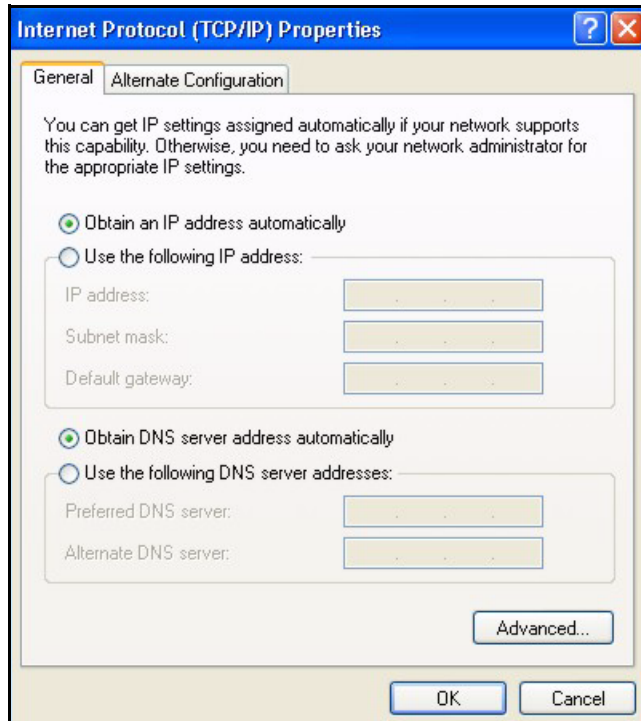
**Figure 78** Windows XP: Local Area Connection Properties

- 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.

- Click **Advanced**.

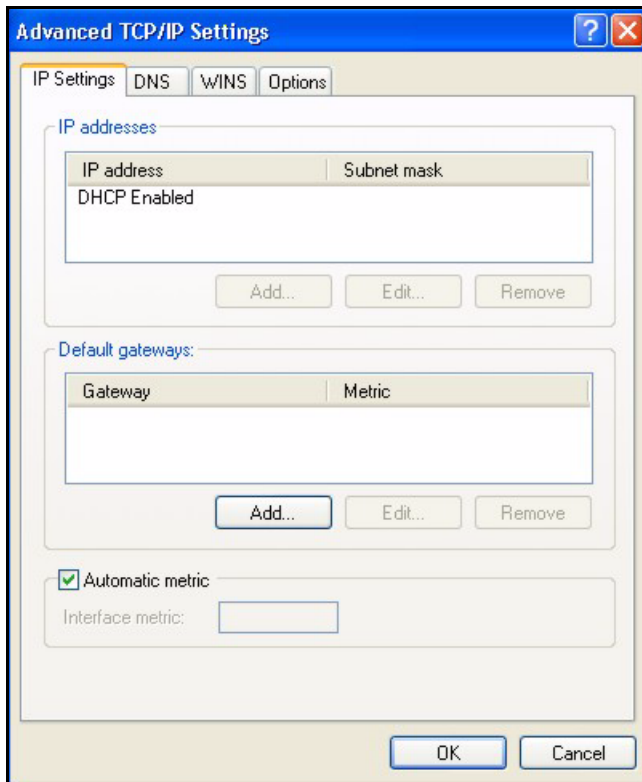
**Figure 79** Windows XP: Internet Protocol (TCP/IP) Properties



- 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:

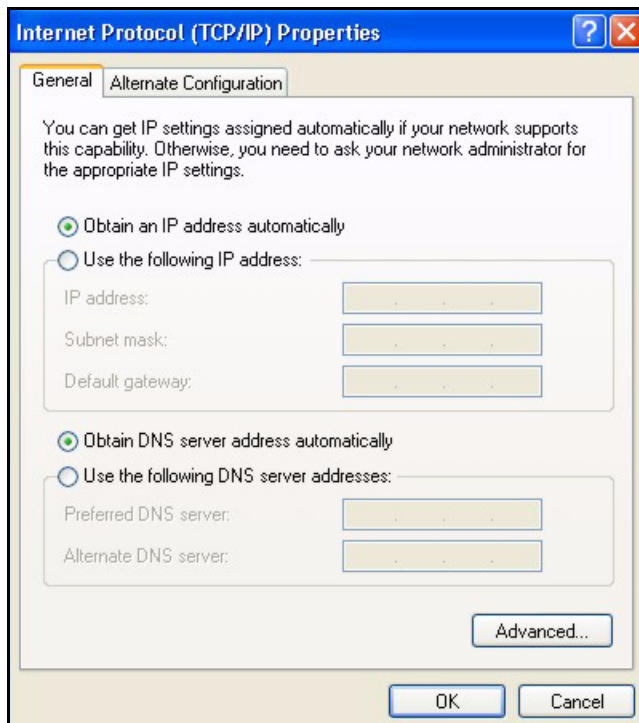
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP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

**Figure 80** 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.

**Figure 81** 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 ZyXEL Device and restart your computer (if prompted).

## Verifying Settings

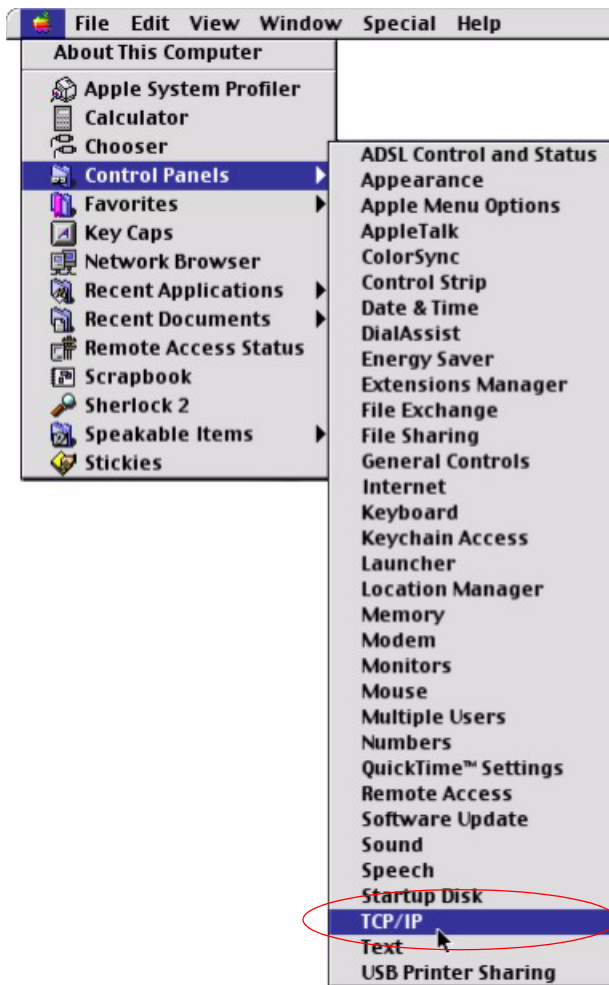
- 1** Click **Start, All Programs, Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

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

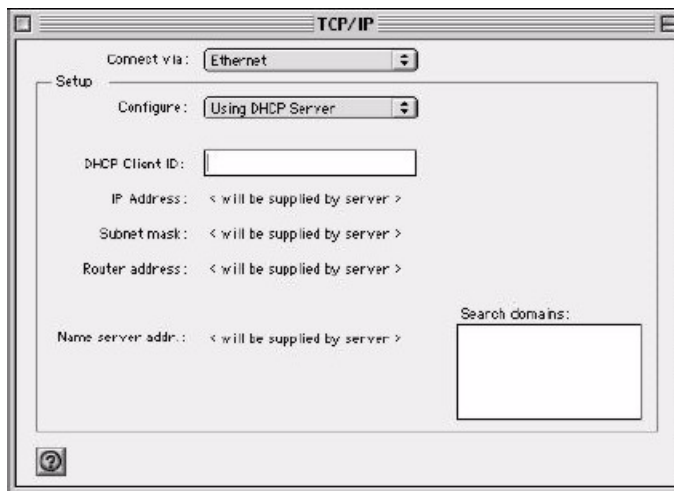


**Figure 82** Macintosh OS 8/9: Apple Menu



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

**Figure 83** Macintosh OS 8/9: TCP/IP



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

- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyXEL Device 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 ZyXEL Device and restart your computer (if prompted).

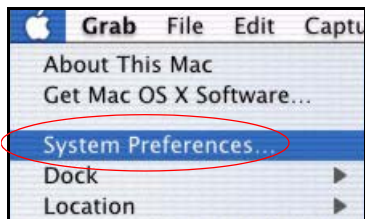
## Verifying Settings

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

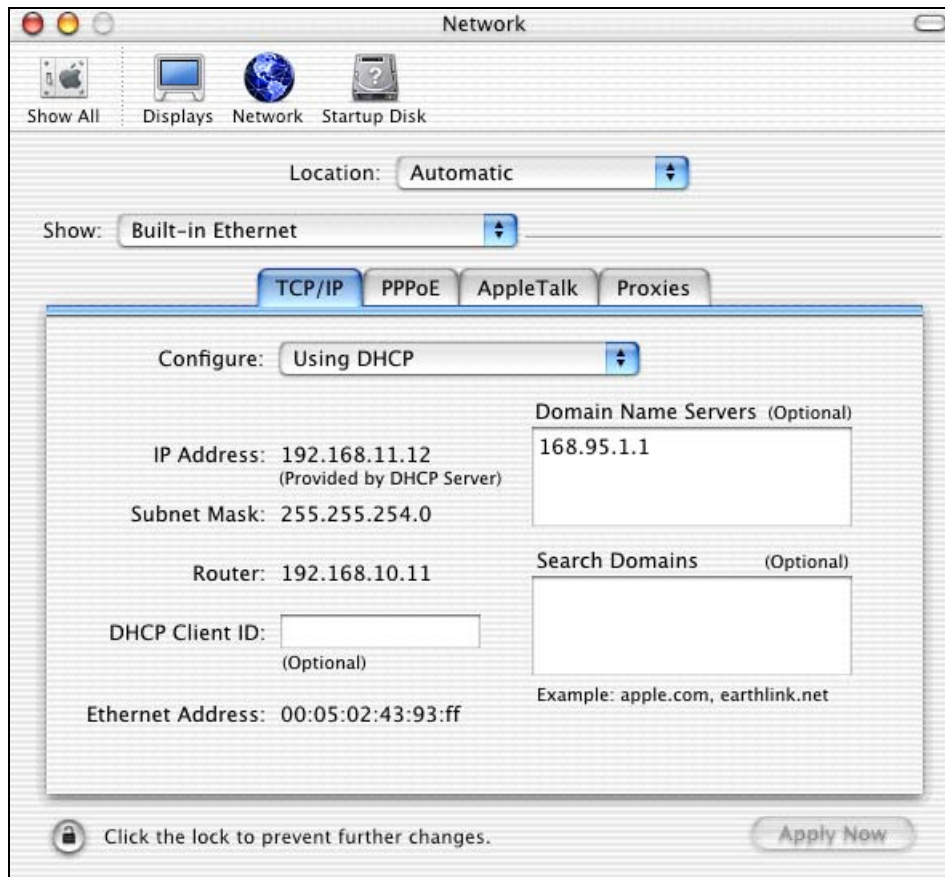
## Macintosh OS X

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

**Figure 84** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 85** 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 ZyXEL Device in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your ZyXEL Device 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.

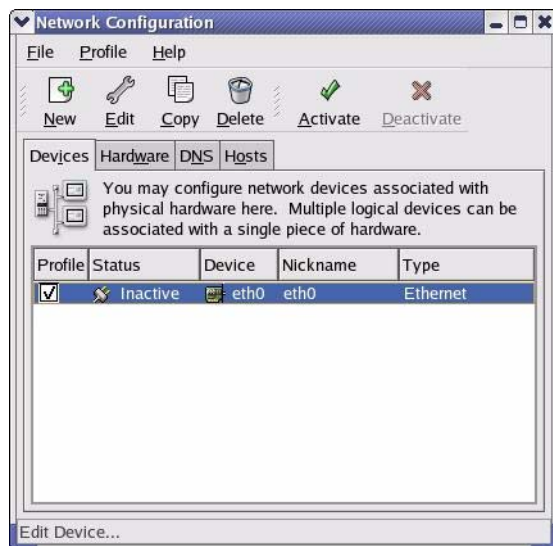
**Note:** Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

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

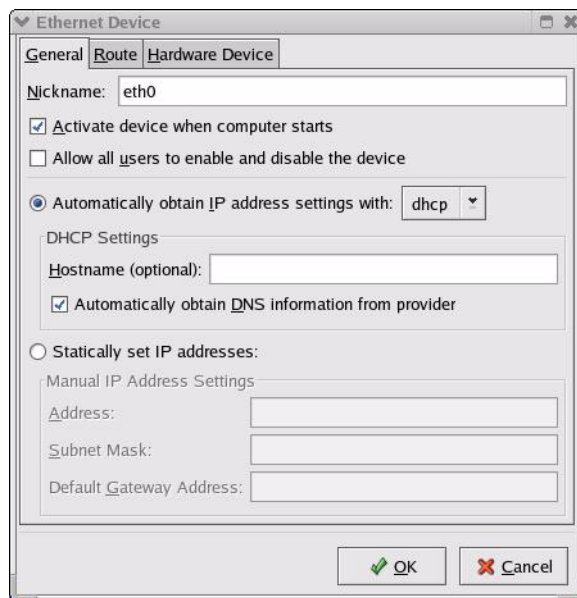
- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 86** Red Hat 9.0: KDE: Network Configuration: Devices



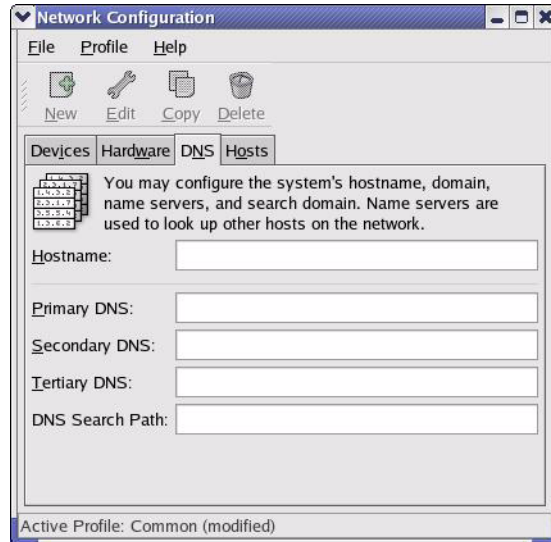
- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 87** Red Hat 9.0: KDE: Ethernet Device: General



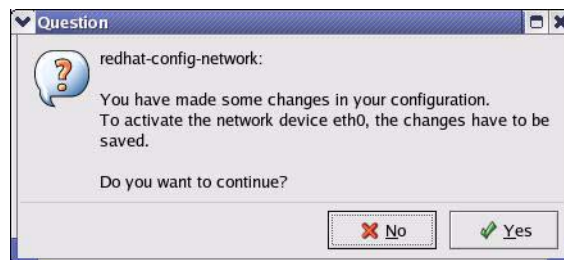
- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
  - If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 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 88** 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 89** 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.

- 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 90** 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 91** 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 92** 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.

**Figure 93** 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 94** 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]#
```

# APPENDIX C

## 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.



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

**Table 45** 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 46** Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239
Class E (reserved)	11110000 to 11111111	240 to 255

## 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 47** “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 48** 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

**Table 48** 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 49** 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 50** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>

**Table 50** 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 51** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
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 (11111111.11111111.11111111.11000000) 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 52** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000

**Table 52** 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 53** Subnet 2

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

**Table 54** Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 55** Subnet 4

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

## Example Eight Subnets

Similarly use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

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

**Table 56** 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 57** 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 45 on page 145](#)) available for subnetting.

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

**Table 58** Class B Subnet Planning

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

## Appendix D

# Splitters and Microfilters

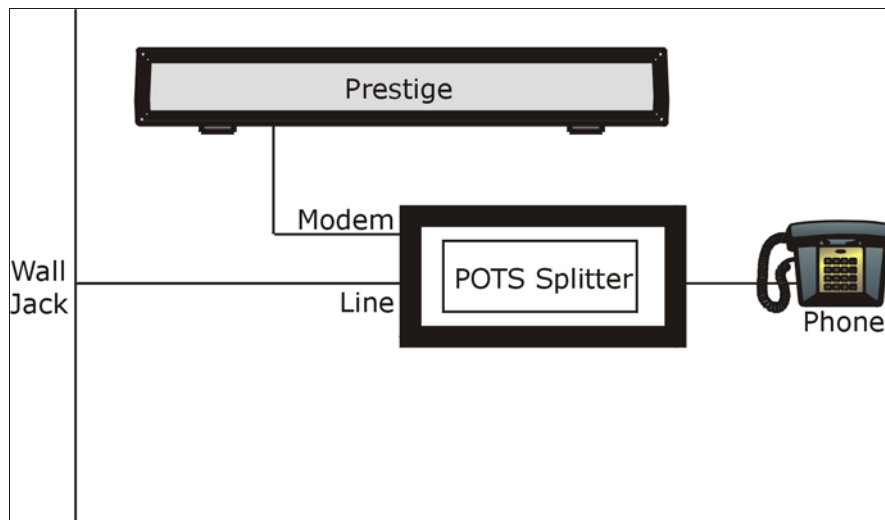
This appendix tells you how to install a POTS splitter or a telephone microfilter.

### Connecting a POTS Splitter

When you use the Full Rate (G.dmt) ADSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitter at the point where the telephone line enters your residence, as shown in the following figure.

**Figure 95** Connecting a POTS Splitter



- 1 Connect the side labeled “Phone” to your telephone.
- 2 Connect the side labeled “Modem” to your ZyXEL Device.
- 3 Connect the side labeled “Line” to the telephone wall jack.

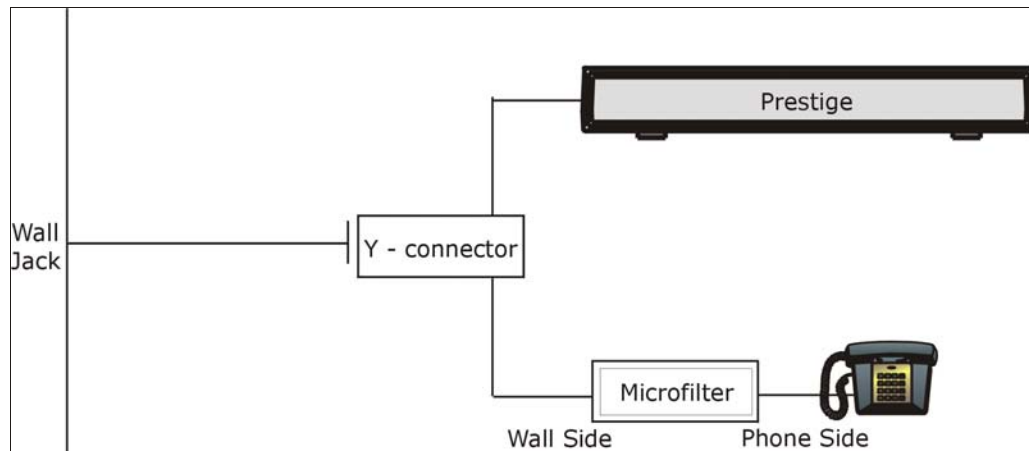
### Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.



- 1 Connect a phone cable from the wall jack to the single jack end of the Y- Connector.
- 2 Connect a cable from the double jack end of the Y-Connector to the “wall side” of the microfilter.
- 3 Connect another cable from the double jack end of the Y-Connector to the ZyXEL Device.
- 4 Connect the “phone side” of the microfilter to your telephone as shown in the following figure.

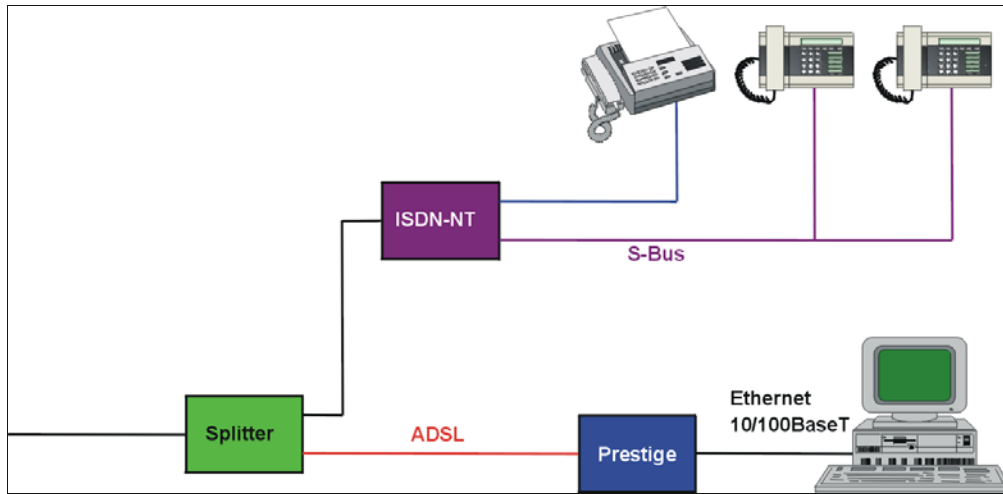
**Figure 96** Connecting a Microfilter



## ZyXEL Device With ISDN

This section relates to people who use their ZyXEL Device with ADSL over ISDN (digital telephone service) only. The following is an example installation for the ZyXEL Device with ISDN.

Figure 97 ZyXEL Device with ISDN





# Appendix E

## Command Interpreter

The following describes how to use the command interpreter. See the included disk or [zyxel.com](http://zyxel.com) for more detailed information on these commands.

**Note:** Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

### Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets `<>`.
- The optional fields in a command are enclosed in square brackets `[ ]`.
- The `|` symbol means or.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

### Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command.



# Appendix F

## Log Descriptions

This appendix provides descriptions of example log messages.

**Table 59** System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP:%s	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns%s	The DHCP server assigned an IP address to a client.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.

**Table 59** System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

**Table 60** System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

**Table 61** Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[TCP   UDP   ICMP   IGMP   Generic] packet filter matched (set:%d, rule:%d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

**Table 62** CDR Logs

LOG MESSAGE	DESCRIPTION
board%d line%d channel%d, call%d,%s C01 Outgoing Call dev=%x ch=%x%s	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID. For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" Means the router has dialed to the PPPoE server 3 times.
board%d line%d channel%d, call%d,%s C02 OutCall Connected%d%s	The PPPoE, PPTP or dial-up call is connected.
board%d line%d channel%d, call%d,%s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

**Table 63** PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

**Table 64** ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded



**Table 64** ICMP Notes (continued)

<b>TYPE</b>	<b>CODE</b>	<b>DESCRIPTION</b>
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

# Appendix G

## PPPoE

### PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see [Figure 98 on page 163](#)). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

### Benefits of PPPoE

PPPoE offers the following benefits:

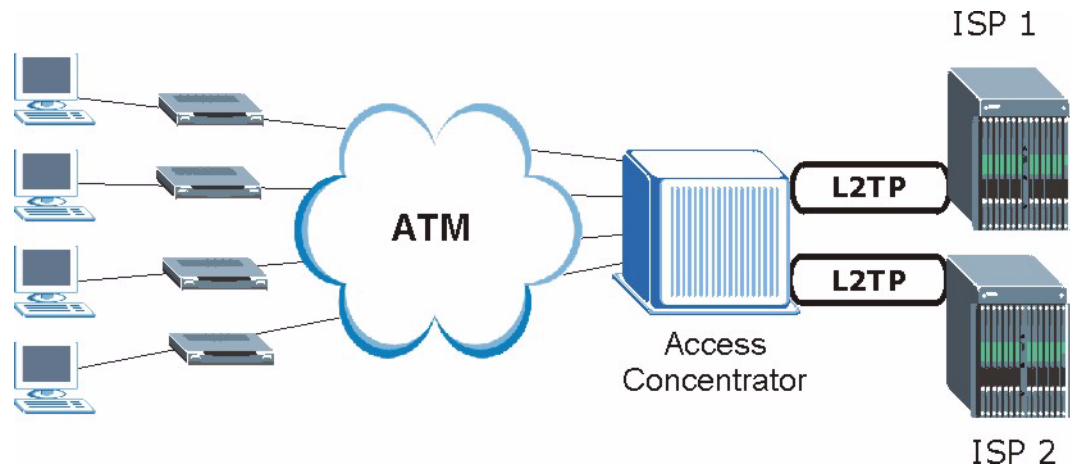
It provides you with a familiar dial-up networking (DUN) user interface.

It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

### Traditional Dial-up Scenario

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

**Figure 98** Single-Computer per Router Hardware Configuration

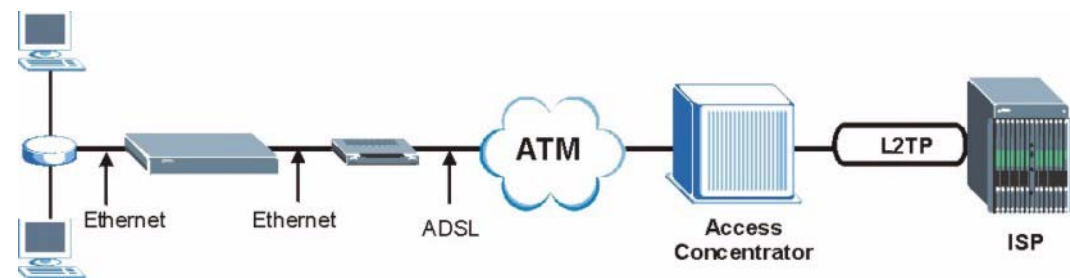
## How PPPoE Works

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

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

## ZyXEL Device as a PPPoE Client

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

**Figure 99** ZyXEL Device as a PPPoE Client

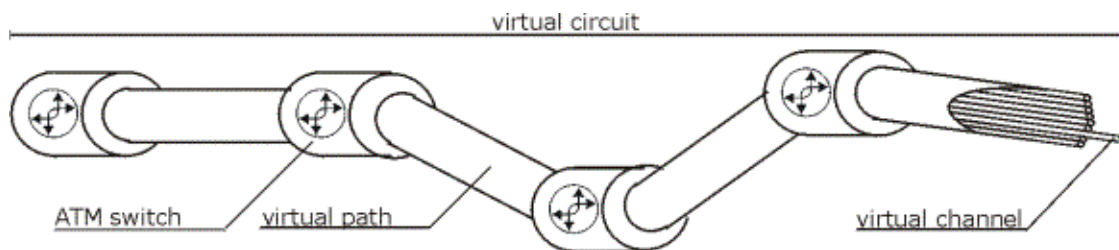
# APPENDIX H

## Virtual Circuit Topology

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel Logical connections between ATM switches
- Virtual Path A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end point

**Figure 100** Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.



# Index

## A

Address Assignment [49](#)  
Address mapping [74](#)  
Address Resolution Protocol (ARP) [52](#)  
ADSLstandards [22](#)  
alternative subnet mask notation [146](#)  
Any IP [23](#), [51](#)  
    How it works [52](#)  
Any IP Setup [54](#)  
Any IP table [102](#)  
applicaions  
    Internet access [27](#)  
ATM Adaptation Layer 5 (AAL5) [34](#)  
auto-Crossover [24](#)  
auto-negotiation [24](#)

## B

Backup [107](#)  
Backup Typ [63](#)

## C

CBR (Continuous Bit Rate) [60](#)  
change password at login [31](#)  
compact [26](#)  
compact guide [30](#)  
Configuration [42](#), [101](#)  
Customer Support [6](#)

## D

Default [109](#)  
default LAN IP address [30](#)  
default user name and password [30](#)  
DHCP [25](#), [42](#), [50](#), [78](#), [101](#)  
DHCP client [25](#)  
DHCP relay [25](#)

DHCP server [25](#), [101](#)  
DHCP table [101](#)  
diagnostic [103](#)  
Domain Name [49](#), [70](#)  
Domain Name System [49](#)  
DSL line, reinitialize [105](#)  
DSLAM (Digital Subscriber Line Access Multiplexer) [27](#)  
Dynamic DNS [24](#), [78](#)  
dynamic DNS [24](#)  
Dynamic Host Configuration Protocol [25](#)  
DYNDNS Wildcard [78](#)

## E

ECHO [70](#)  
embedded help [32](#)  
Encapsulated Routing Link Protocol (ENET ENCAP) [34](#)  
Encapsulation [25](#), [34](#)  
    ENET ENCAP [34](#)  
    PPP over Ethernet [34](#)  
    PPPoA [34](#)  
    RFC 1483 [35](#)  
encapsulation [25](#)  
Ethernet [125](#)

## F

Factory Defaults [109](#)  
Factory LAN Defaults [50](#)  
faulty Ethernet cables [112](#)  
FCC [3](#)  
Federal Communications Commission [3](#)  
Finger [70](#)  
firmware [105](#)  
    upload [105](#)  
    upload error [107](#)  
Frame Relay [27](#)  
FTP [70](#), [82](#)  
FTP Restrictions [82](#)  
Full Rate [152](#)

## G

Graphical User Interface (GUI) [22](#)

## H

hardware problem [112](#)

Host [46](#)

HTTP [71](#)

HTTP (Hypertext Transfer Protocol) [105](#)

## I

IANA [38](#)

IGMP [51](#)

Install UPnP [88](#)

Windows Me [88](#)

Windows XP [90](#)

Internet Access [22](#), [27](#)

Internet access [34](#)

Internet Access Setup [114](#)

Internet access wizard setup [35](#)

Internet Assigned Numbers AuthoritySee IANA [38](#)

IP Address [36](#), [50](#), [70](#), [101](#)

IP Address Assignment [37](#)

ENET ENCAP [37](#)

PPPoA or PPPoE [37](#)

RFC 1483 [37](#)

IP alias [25](#)

IP Policy Routing (IPPR) [25](#)

IP Pool Setup [42](#)

## L

LAN Setup [48](#), [56](#)

LAN TCP/IP [50](#)

LEDs [112](#)

## M

MAC (Media Access Control) [102](#)

maintenance [98](#)

management idle timeout period [31](#)

Maximum Burst Size (MBS) [57](#), [60](#)

MDI/MDI-X [24](#)

Metric [56](#)

Multicast [51](#)

Multiplexing [25](#), [35](#)

multiplexing [25](#), [35](#)

LLC-based [35](#)

VC-based [35](#)

Multiprotocol Encapsulation [35](#)

## N

Nailed-Up Connection [38](#)

NAT [37](#), [70](#), [71](#)

Address mapping rule [75](#)

Application [68](#)

Definitions [66](#)

How it works [67](#)

Mapping Types [68](#)

What it does [67](#)

What NAT does [67](#)

NAT (Network Address Translation) [66](#)

NAT mode [72](#)

NAT Traversal [86](#)

navigating the web configurator [32](#)

Network Address Translation (NAT) [23](#)

Network Management [25](#), [71](#)

NNTP [71](#)

## P

Password [46](#)

password [113](#)

Peak Cell Rate (PCR) [57](#), [60](#)

Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [34](#)

Point-to-Point Tunneling Protocol [71](#)

POP3 [71](#)

Port Numbers [70](#)

power [112](#)

PPP session over Ethernet (PPP over Ethernet, RFC 2516) [34](#)

PPPoE [57](#), [162](#)

Benefits [57](#)

PPPoE (Point-to-Point Protocol over Ethernet) [23](#), [57](#)

PPTP [71](#)

PVC (Permanent Virtual Circuit) [34](#)

**Q**

Quick Start Guide [20](#)

**R**

reinitialize the ADSL line [105](#)  
 Related Documentation [20](#)  
 remote management [114](#)  
 Remote Management and NAT [83](#)  
 Remote Management Limitations [82](#)  
 Reset button, the [32](#)  
 resetting the Prestige [32](#)  
 Restore [108](#)  
 RFC 1483 [35](#)  
 RFC 1631 [66](#)  
 RFC2516 [23](#)  
 RIPSee Routing Information Protocol [50](#)  
 Routing Information Protocol [50](#)  
   Direction [50](#)  
   Version [50](#)

**S**

Server [69](#)  
 Service Type [114](#)  
 Services [70](#)  
 Single User Account (SUA) [27](#)  
 SMTP [70](#)  
 SNMP [71](#)  
 SOHO (Small Office/Home Office) [27](#)  
 Splitters [152](#)  
 SUA [69, 71](#)  
 SUA (Single User Account) [69](#)  
 SUA server [70, 72](#)  
   Default server set [70](#)  
 SUA vs NAT [69](#)  
 SUA/NAT Server Set [73](#)  
 subnet [144](#)  
 Subnet Mask [36, 50](#)  
 subnet mask [146](#)  
 subnetting [146](#)  
 Supporting Disk [20](#)  
 Sustain Cell Rate (SCR) [60](#)  
 Sustained Cell Rate (SCR) [57](#)  
 Syntax Conventions [20](#)

System Timeout [83](#)

**T**

TCP/IP [83](#)  
 Telnet [83](#)  
 Telnet Configuration [83](#)  
 TFTP Restrictions [82](#)  
 Traffic Redirect [61, 62](#)  
 Traffic redirect [61](#)  
 traffic redirect [23](#)  
 Traffic shaping [57](#)

**U**

UBR (Unspecified Bit Rate) [60](#)  
 Universal Plug and Play [86](#)  
   Application [86](#)  
 Universal Plug and Play (UPnP) [23](#)  
 UPnP [86](#)  
   Forum [87](#)  
   security issues [87](#)  
 User Name [79](#)

**V**

VBR (Variable Bit Rate) [60](#)  
 Virtual Channel Identifier (VCI) [35](#)  
 virtual circuit (VC) [35](#)  
 Virtual Path Identifier (VPI) [35](#)  
 VPI & VCI [35](#)

**W**

WAN (Wide Area Network) [56](#)  
 WAN backup [62](#)  
 Web Configurator [30, 32](#)  
 web configurator screen summary [32](#)  
 web service [115](#)



## Z

Zero Configuration Internet Access [23](#)