

P-335 Plus

Firewall Router with USB Print Server

User's Guide

Version 3.60
Edition 1
8/2006

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is lowercase and the "XEL" is uppercase. The letters are closely spaced and have a slight shadow effect.

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 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

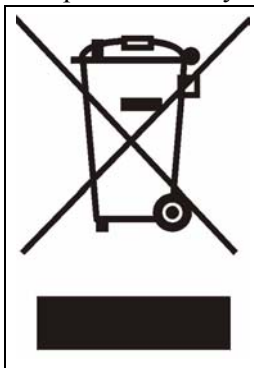
- 1 Go to <http://www.zyxel.com>.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

Safety Warnings

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

- 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 store things on the device.
- Connect ONLY suitable accessories to the device.

This product is recyclable. Dispose of it properly.



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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been 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 to the purchaser.

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

Registration

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

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

Copyright	3
Certifications	4
Safety Warnings	5
ZyXEL Limited Warranty	6
Customer Support.....	7
Table of Contents	9
Preface	25
Chapter 1	
Getting to Know Your ZyXEL Device.....	27
1.1 Overview	27
1.1.1 Print Server	27
1.1.2 Print Server and Router Combined	28
1.2 Good Habits for Managing Your ZyXEL Device	28
1.3 Front Panel LEDs	29
Chapter 2	
Introducing the Web Configurator.....	31
2.1 Web Configurator Overview	31
2.2 Accessing the Web Configurator	31
2.3 Resetting the ZyXEL Device	32
2.3.1 Procedure to Use the Reset Button	32
2.4 Navigating the Web Configurator	32
2.4.1 Router Mode Status	32
2.4.2 Print Server Mode Status	35
2.4.3 Navigation Panel	37
2.4.4 Summary: Bandwidth Management Monitor	39
2.4.5 Summary: DHCP Table	40
2.4.6 Summary: Packet Statistics	40
Chapter 3	
Connection Wizard.....	43
3.1 Wizard Setup	43
3.2 Connection Wizard: STEP 1: System Information	44
3.2.1 System Name	44

3.2.2 Domain Name	45
3.3 Connection Wizard: STEP 2: Internet Configuration	45
3.3.1 Ethernet Connection	46
3.3.2 PPPoE Connection	47
3.3.3 PPTP Connection	48
3.3.4 Your IP Address	49
3.3.5 WAN IP Address Assignment	50
3.3.6 IP Address and Subnet Mask	50
3.3.7 DNS Server Address Assignment	51
3.3.8 WAN IP and DNS Server Address Assignment.....	51
3.3.9 WAN MAC Address	53
3.4 Connection Wizard: STEP 3: Bandwidth management	54
3.5 Connection Wizard Complete	54
Chapter 4	
WAN.....	57
4.1 WAN Overview	57
4.2 WAN MAC Address	57
4.3 Internet Connection	57
4.3.1 Ethernet Encapsulation	57
4.3.2 PPPoE Encapsulation	59
4.3.3 PPTP Encapsulation	62
4.4 Advanced WAN Screen	65
Chapter 5	
LAN.....	67
5.1 LAN Overview	67
5.1.1 IP Pool Setup	67
5.1.2 System DNS Servers	67
5.2 LAN TCP/IP	67
5.2.1 Factory LAN Defaults	67
5.2.2 IP Address and Subnet Mask	68
5.2.3 Multicast	68
5.3 LAN IP Screen	68
5.4 LAN IP Alias	69
5.5 Advanced LAN Screen	70
Chapter 6	
DHCP Server.....	73
6.1 DHCP	73
6.2 DHCP Server General Screen	73
6.3 DHCP Server Advanced Screen	74
6.4 Client List Screen	75

Chapter 7	
Network Address Translation (NAT)	77
7.1 NAT Overview	77
7.2 Using NAT	77
7.2.1 Port Forwarding: Services and Port Numbers	77
7.2.2 Configuring Servers Behind Port Forwarding (Example)	78
7.3 General NAT Screen	78
7.4 NAT Application Screen	79
7.4.1 Game List Example	81
7.5 Trigger Port Forwarding	82
7.5.1 Trigger Port Forwarding Example	83
7.5.2 Two Points To Remember About Trigger Ports	83
7.6 NAT Advanced Screen	83
Chapter 8	
Dynamic DNS	87
8.1 Dynamic DNS Introduction	87
8.1.1 DynDNS Wildcard	87
8.2 Dynamic DNS Screen	87
Chapter 9	
Firewall	89
9.1 Introduction to Firewall	89
9.1.1 What is a Firewall?	89
9.1.2 Stateful Inspection Firewall	89
9.1.3 About the ZyXEL Device Firewall	89
9.1.4 Guidelines For Enhancing Security With Your Firewall	90
9.2 Triangle Routes	90
9.2.1 Triangle Routes and IP Alias	91
9.3 General Firewall Screen	91
9.4 Services Screen	92
Chapter 10	
Content Filtering	95
10.1 Introduction to Content Filtering	95
10.2 Restrict Web Features	95
10.3 Days and Times	95
10.4 Filter Screen	95
10.5 Schedule	97
10.6 Customizing Keyword Blocking URL Checking	98
10.6.1 Domain Name or IP Address URL Checking	98
10.6.2 Full Path URL Checking	98
10.6.3 File Name URL Checking	99

Chapter 11	
Static Route Screens	101
11.1 Static Route Overview	101
11.2 IP Static Route Screen	102
11.2.1 Static Route Setup Screen	103
Chapter 12	
Bandwidth Management	105
12.1 Bandwidth Management Overview	105
12.2 Application-based Bandwidth Management	105
12.3 Subnet-based Bandwidth Management	105
12.4 Application and Subnet-based Bandwidth Management	106
12.5 Bandwidth Management Priorities	107
12.6 Predefined Bandwidth Management Services	107
12.6.1 Services and Port Numbers	108
12.7 Default Bandwidth Management Classes and Priorities	110
12.8 Bandwidth Management General Configuration	111
12.9 Bandwidth Management Advanced Configuration	112
12.9.1 Rule Configuration with the Pre-defined Service	114
12.9.2 Rule Configuration with the User-defined Service	115
12.10 Bandwidth Management Monitor	116
Chapter 13	
Remote Management Screens	117
13.1 Remote Management Overview	117
13.1.1 Remote Management Limitations	117
13.1.2 Remote Management and NAT	118
13.1.3 System Timeout	118
13.2 WWW Screen	118
13.3 Telnet	119
13.4 Telnet Screen	120
13.5 FTP Screen	120
13.6 DNS Screen	121
Chapter 14	
UPnP	123
14.1 Universal Plug and Play Overview	123
14.1.1 How Do I Know If I'm Using UPnP?	123
14.1.2 NAT Traversal	123
14.1.3 Cautions with UPnP	123
14.2 UPnP and ZyXEL	124
14.3 UPnP Screen	124
14.4 Installing UPnP in Windows Example	125

14.4.1 Installing UPnP in Windows Me	125
14.4.2 Installing UPnP in Windows XP	126
14.5 Using UPnP in Windows XP Example	127
14.5.1 Auto-discover Your UPnP-enabled Network Device	127
14.5.2 Web Configurator Easy Access	128
14.5.3 Web Configurator Easy Access	129
Chapter 15	
Print Server	131
15.1 Print Server Overview	131
15.2 ZyXEL Device Print Server	131
15.3 Print Server Screen	132
Chapter 16	
Print Server Driver Setup	133
16.1 Installation Requirements	133
16.2 Windows 95/98 SE/Me/2000/XP/NT 4.0	133
16.2.1 Print Server Driver Setup Wizard	134
16.2.2 Adding a New Printer	139
16.3 Macintosh OS X	143
Chapter 17	
System	147
17.1 System Overview	147
17.2 System General Screen	147
17.3 Time Setting Screen	148
Chapter 18	
Logs.....	151
18.1 View Log	151
18.2 Log Settings	152
Chapter 19	
Tools.....	155
19.1 Firmware Upload Screen	155
19.2 Configuration Screen	156
19.2.1 Backup Configuration	157
19.2.2 Restore Configuration	157
19.2.3 Back to Factory Defaults	158
19.3 Restart Screen	159

Chapter 20	
Configuration Mode	161
Chapter 21	
Troubleshooting	163
21.1 Problems Starting Up the ZyXEL Device	163
21.2 Problems with the LAN	163
21.3 Problems with the WAN	164
21.4 Problems with Restricted Web Pages and Keyword Blocking	164
21.5 Problems with the Password	165
21.6 Problems with the Print Server	165
21.7 Problems with Remote Management	166
21.8 Problems Accessing the ZyXEL Device	166
21.8.1 Pop-up Windows, JavaScripts and Java Permissions	166
21.8.1.1 Internet Explorer Pop-up Blockers	167
21.8.1.2 JavaScripts	170
21.8.1.3 Java Permissions	172
21.8.2 ActiveX Controls in Internet Explorer	174
Appendix A	
Product Specifications	177
Appendix B	
Print Server Specifications	179
Appendix C	
Setting up Your Computer's IP Address.....	185
Appendix D	
IP Addresses and Subnetting	201
Appendix E	
Command Interpreter.....	209
Appendix F	
Log Descriptions.....	211
Appendix G	
NetBIOS Filter Commands	221
Appendix H	
Services	223
Appendix I	
Wall-mounting Instructions.....	227
Appendix J	

Internal SPTGEN 229

List of Figures

Figure 1 ZyXEL Device as a Print Server	27
Figure 2 ZyXEL Device as a Print Server and Router Combined	28
Figure 3 Front Panel	29
Figure 4 Change Password Screen	32
Figure 5 Web Configurator Status Screen (Router Mode)	33
Figure 6 Web Configurator Status Screen (Print Server Mode)	35
Figure 7 Summary: BW MGMT Monitor	39
Figure 8 Summary: DHCP Table	40
Figure 9 Summary: Packet Statistics	41
Figure 10 Select Wizard or Advanced Mode	43
Figure 11 Select a Language	44
Figure 12 Welcome to the Connection Wizard	44
Figure 13 Wizard Step 1: System Information	45
Figure 14 Wizard Step 3: ISP Parameters.	46
Figure 15 Wizard Step 2: Ethernet Connection	46
Figure 16 Wizard Step 2: PPPoE Connection	47
Figure 17 Wizard Step 2: PPTP Connection	48
Figure 18 Wizard Step 2: Your IP Address	49
Figure 19 Wizard Step 2: WAN IP and DNS Server Addresses	52
Figure 20 Wizard Step 2: WAN MAC Address	53
Figure 21 Wizard Step 3: Bandwidth Management	54
Figure 22 Connection Wizard Complete	55
Figure 23 Ethernet Encapsulation	58
Figure 24 PPPoE Encapsulation	60
Figure 25 PPTP Encapsulation	63
Figure 26 Advanced	65
Figure 27 LAN IP	68
Figure 28 LAN IP Alias	69
Figure 29 Advanced LAN	70
Figure 30 DHCP Server General	73
Figure 31 DHCP Server Advanced	74
Figure 32 Client List	76
Figure 33 Multiple Servers Behind NAT Example	78
Figure 34 NAT General	78
Figure 35 NAT Application	80
Figure 36 Game List Example	82

Figure 37 Trigger Port Forwarding Process: Example	83
Figure 38 NAT Advanced	84
Figure 39 Dynamic DNS	88
Figure 40 Using IP Alias to Solve the Triangle Route Problem	91
Figure 41 General	91
Figure 42 Services	93
Figure 43 Content Filter: Filter	96
Figure 44 Content Filter: Schedule	97
Figure 45 Example of Static Routing Topology	101
Figure 46 IP Static Route	102
Figure 47 Static Route Setup	103
Figure 48 Subnet-based Bandwidth Management Example	106
Figure 49 Bandwidth Management: General	111
Figure 50 Bandwidth Management: Advanced	112
Figure 51 Bandwidth Management Rule Configuration: Pre-defined Service	114
Figure 52 Bandwidth Management Rule Configuration: User-defined Service	115
Figure 53 Bandwidth Management: Monitor	116
Figure 54 WWW Remote Management	118
Figure 55 Telnet Configuration on a TCP/IP Network	119
Figure 56 Telnet Remote Management	120
Figure 57 FTP Remote Management	121
Figure 58 DNS Remote Management	122
Figure 59 Configuring UPnP	124
Figure 60 Configuring Print Server	132
Figure 61 CD Autorun Screen	133
Figure 62 CD Autorun Screen: Printer Server Driver Setup	134
Figure 63 Network Print Server Setup Wizard: Welcome	135
Figure 64 Network Print Server Setup Wizard: Select A Print Server	135
Figure 65 Network Print Server Setup Wizard: Change Settings	136
Figure 66 Network Print Server Setup Wizard: Select A Printer	137
Figure 67 Network Print Server Setup Wizard: Summary	138
Figure 68 Network Print Server Setup Wizard: Installation Complete	138
Figure 69 Add Printer Help	139
Figure 70 Add Printer Wizard: Welcome	139
Figure 71 Add Printer Wizard: Local or Network Printer	140
Figure 72 Add Printer Wizard: Select the Printer Port	140
Figure 73 Add Printer Wizard: Printer Driver	141
Figure 74 Add Printer Wizard: Use Existing Driver	141
Figure 75 Add Printer Wizard: Name Your Printer	142
Figure 76 Add Printer Wizard: Printer Sharing	142
Figure 77 Add Printer Wizard: Print Test Page	143
Figure 78 Add Printer Wizard Complete	143
Figure 79 Macintosh HD	144

Figure 80 Macintosh HD folder	144
Figure 81 Applications Folder	144
Figure 82 Utilities Folder	144
Figure 83 Printer List Folder	145
Figure 84 Printer Configuration	145
Figure 85 Printer Model	146
Figure 86 Print Server	146
Figure 87 System General	147
Figure 88 Time Setting	149
Figure 89 View Log	151
Figure 90 Log Settings	153
Figure 91 Maintenance Firmware Upload	155
Figure 92 Upload Warning	156
Figure 93 Network Temporarily Disconnected	156
Figure 94 Upload Error Message	156
Figure 95 Configuration	157
Figure 96 Configuration Restore Successful	158
Figure 97 Temporarily Disconnected	158
Figure 98 Configuration Restore Error	158
Figure 99 System Restart	159
Figure 100 Config Mode	161
Figure 101 Pop-up Blocker	167
Figure 102 Internet Options	168
Figure 103 Internet Options	169
Figure 104 Pop-up Blocker Settings	170
Figure 105 Internet Options	171
Figure 106 Security Settings - Java Scripting	172
Figure 107 Security Settings - Java	173
Figure 108 Java (Sun)	174
Figure 109 Internet Options Security	175
Figure 110 Security Setting ActiveX Controls	176
Figure 111 Windows 95/98/Me: Network: Configuration	186
Figure 112 Windows 95/98/Me: TCP/IP Properties: IP Address	187
Figure 113 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	188
Figure 114 Windows XP: Start Menu	189
Figure 115 Windows XP: Control Panel	189
Figure 116 Windows XP: Control Panel: Network Connections: Properties	190
Figure 117 Windows XP: Local Area Connection Properties	190
Figure 118 Windows XP: Internet Protocol (TCP/IP) Properties	191
Figure 119 Windows XP: Advanced TCP/IP Properties	192
Figure 120 Windows XP: Internet Protocol (TCP/IP) Properties	193
Figure 121 Macintosh OS 8/9: Apple Menu	194
Figure 122 Macintosh OS 8/9: TCP/IP	194

Figure 123 Macintosh OS X: Apple Menu	195
Figure 124 Macintosh OS X: Network	196
Figure 125 Red Hat 9.0: KDE: Network Configuration: Devices	197
Figure 126 Red Hat 9.0: KDE: Ethernet Device: General	197
Figure 127 Red Hat 9.0: KDE: Network Configuration: DNS	198
Figure 128 Red Hat 9.0: KDE: Network Configuration: Activate	198
Figure 129 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	199
Figure 130 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	199
Figure 131 Red Hat 9.0: DNS Settings in resolv.conf	199
Figure 132 Red Hat 9.0: Restart Ethernet Card	200
Figure 133 Red Hat 9.0: Checking TCP/IP Properties	200
Figure 134 Displaying Log Categories Example	219
Figure 135 Displaying Log Parameters Example	219
Figure 136 Wall-mounting Example	227
Figure 137 Configuration Text File Format: Column Descriptions	229
Figure 138 Invalid Parameter Entered: Command Line Example	230
Figure 139 Valid Parameter Entered: Command Line Example	230
Figure 140 Internal SPTGEN FTP Download Example	231
Figure 141 Internal SPTGEN FTP Upload Example	231

List of Tables

Table 1 Front Panel LEDs	29
Table 2 Status Screen Icon Key	33
Table 3 Web Configurator Status Screen (Router Mode)	34
Table 4 Status Screen Icon Key	36
Table 5 Web Configurator Status Screen (Print Server Mode)	36
Table 6 Router and Print Server Mode Features Comparison	37
Table 7 Screens Summary	38
Table 8 Summary: DHCP Table	40
Table 9 Summary: Packet Statistics	41
Table 10 Wizard Step 1: System Information	45
Table 11 Wizard Step 2: ISP Parameters	46
Table 12 Wizard Step 2: PPPoE Connection	47
Table 13 Wizard Step 2: PPTP Connection	49
Table 14 Wizard Step 2: Your IP Address	50
Table 15 Private IP Address Ranges	50
Table 16 Wizard Step 2: WAN IP and DNS Server Addresses	52
Table 17 Example of Network Properties for LAN Servers with Fixed IP Addresses	53
Table 18 Wizard Step 2: WAN MAC Address	53
Table 19 Wizard Step 3: Bandwidth Management	54
Table 20 Ethernet Encapsulation	58
Table 21 PPPoE Encapsulation	61
Table 22 PPTP Encapsulation	64
Table 23 Advanced	66
Table 24 LAN IP	69
Table 25 LAN IP Alias	70
Table 26 Advanced LAN	70
Table 27 DHCP Server General	73
Table 28 DHCP Server Advanced	75
Table 29 Client List	76
Table 30 NAT General	79
Table 31 NAT Application	80
Table 32 NAT Advanced	84
Table 33 Dynamic DNS	88
Table 34 Firewall General	92
Table 35 Firewall Services	93
Table 36 Content Filter: Filter	96

Table 37 Content Filter: Schedule	98
Table 38 IP Static Route	102
Table 39 Static Route Setup	103
Table 40 Application and Subnet-based Bandwidth Management Example	106
Table 41 Bandwidth Management Priorities	107
Table 42 Media Bandwidth Management Setup: Services	107
Table 43 Commonly Used Services	108
Table 44 Bandwidth Management Priority with Default Classes	110
Table 45 Bandwidth Management: General	111
Table 46 Bandwidth Management: Advanced	113
Table 47 Bandwidth Management Rule Configuration: Pre-defined Service	114
Table 48 Bandwidth Management Rule Configuration: User-defined Service	115
Table 49 WWW Remote Management	118
Table 50 Telnet Remote Management	120
Table 51 FTP Remote Management	121
Table 52 DNS Remote Management	122
Table 53 Configuring UPnP	125
Table 54 Configuring Print Server	132
Table 55 System General	148
Table 56 Time Setting	149
Table 57 View Logs	152
Table 58 Log Settings	153
Table 59 Maintenance Firmware Upload	155
Table 60 Maintenance Restore Configuration	157
Table 61 Config Mode: Advanced Screens	161
Table 62 Troubleshooting Starting Up Your ZyXEL Device	163
Table 63 Troubleshooting the LAN	163
Table 64 Troubleshooting the WAN	164
Table 65 Troubleshooting Restricted Web Pages and Keyword Blocking	164
Table 66 Troubleshooting the Password	165
Table 67 Troubleshooting the Print Server	165
Table 68 Troubleshooting Telnet	166
Table 69 Troubleshooting Accessing the ZyXEL Device	166
Table 70 Hardware Features	177
Table 71 Firmware Features	177
Table 72 Print Server Interface	179
Table 73 Print Server Requirements and Specifications	179
Table 74 Compatible USB Printers	180
Table 75 Classes of IP Addresses	202
Table 76 Allowed IP Address Range By Class	202
Table 77 "Natural" Masks	203
Table 78 Alternative Subnet Mask Notation	203
Table 79 Two Subnets Example	204

Table 80 Subnet 1	204
Table 81 Subnet 2	205
Table 82 Subnet 1	205
Table 83 Subnet 2	206
Table 84 Subnet 3	206
Table 85 Subnet 4	206
Table 86 Eight Subnets	207
Table 87 Class C Subnet Planning	207
Table 88 Class B Subnet Planning	208
Table 89 System Maintenance Logs	211
Table 90 System Error Logs	212
Table 91 Access Control Logs	212
Table 92 TCP Reset Logs	213
Table 93 Packet Filter Logs	213
Table 94 ICMP Logs	214
Table 95 CDR Logs	214
Table 96 PPP Logs	214
Table 97 UPnP Logs	215
Table 98 Content Filtering Logs	215
Table 99 Attack Logs	216
Table 100 ACL Setting Notes	217
Table 101 ICMP Notes	217
Table 102 Syslog Logs	218
Table 103 RFC-2408 ISAKMP Payload Types	218
Table 104 NetBIOS Filter Default Settings	222
Table 105 Examples of Services	223
Table 106 Abbreviations Used in the Example Internal SPTGEN Screens Table	232
Table 107 Menu 1 General Setup	232
Table 108 Menu 3	232
Table 109 Menu 4 Internet Access Setup	236
Table 110 Menu 12	237
Table 111 Menu 15 SUA Server Setup	238
Table 112 Menu 21.1 Filter Set #1	239
Table 113 Menu 21.1 Filer Set #2,	241
Table 114 Menu 23 System Menus	242
Table 115 Menu 24.11 Remote Management Control	243
Table 116 Command Examples	244

Preface

Congratulations on your purchase of the P-335 Plus Firewall Router with USB Print Server. This manual is designed to guide you through the configuration of your P-335 Plus for its various applications.

About This User's Guide

This User's Guide is designed to guide you through the configuration of your ZyXEL Device using the web configurator.

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

Related Documentation

- Supporting Disk
Refer to the included CD for support documents.
- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. They contain connection information and instructions on getting started.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Web Site
Please go to <http://www.zyxel.com> for product news, firmware, updated documents, and other support materials.










User Guide Feedback

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

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choice.
- Mouse action sequences are denoted using a right angle bracket (>). For example, “In Windows, click **Start** > **Settings** > **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-335 Plus series may be referred to as the “ZyXEL Device” in this User's Guide.

Graphics Icons Key

ZyXEL Device 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Modem 	Switch 	Router 

CHAPTER 1

Getting to Know Your ZyXEL Device

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

1.1 Overview

This ZyXEL Device is a secure router with a 4-port switch and print server.

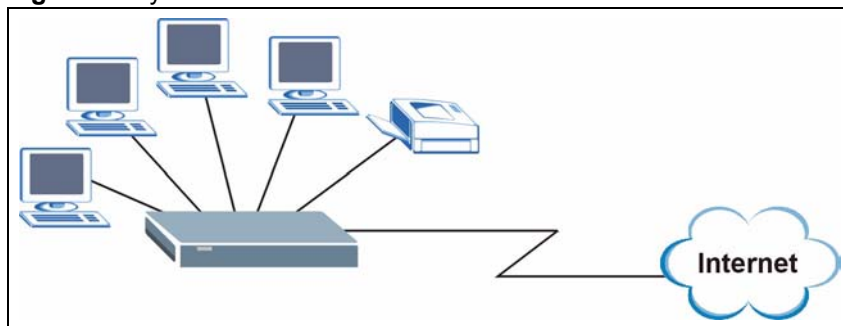
Typical uses for the ZyXEL Device are as a print server or as a print server and router combined. When you use it as a print server, you don't have to make any configuration changes to your existing network. When you use it as a print server and router combined, you can take advantage of a host of features such as firewall, content filtering and bandwidth management.

See [Appendix A on page 177](#) for a complete list of features you can configure on your ZyXEL Device.

1.1.1 Print Server

The ZyXEL Device's print server allows your network's computers to share a printer. Simply connect a USB printer to the USB port on the ZyXEL Device. To disable routing functions, put the **PR** switch to the **P** position.

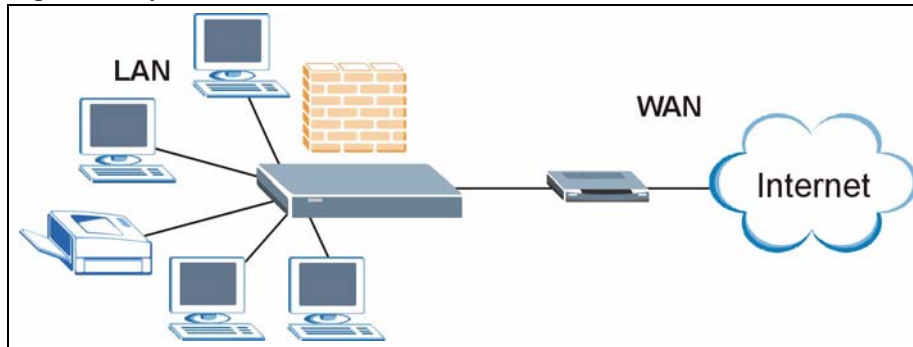
Figure 1 ZyXEL Device as a Print Server



1.1.2 Print Server and Router Combined

For Internet access, connect the WAN Ethernet port to your existing Internet access gateway (company network, or your cable or DSL modem for example). Connect computers or servers to the LAN ports for shared Internet access. See the Quick Start Guide for instructions on hardware connections.

Figure 2 ZyXEL Device as a Print Server and Router Combined



You can also configure firewall and content filtering on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.

Use content filtering to block access to web sites containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to certain web sites for the kids.

Use bandwidth management to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that voice over Internet calls get enough bandwidth in your network, and/or limit bandwidth devoted to the boss's excessive file downloading.

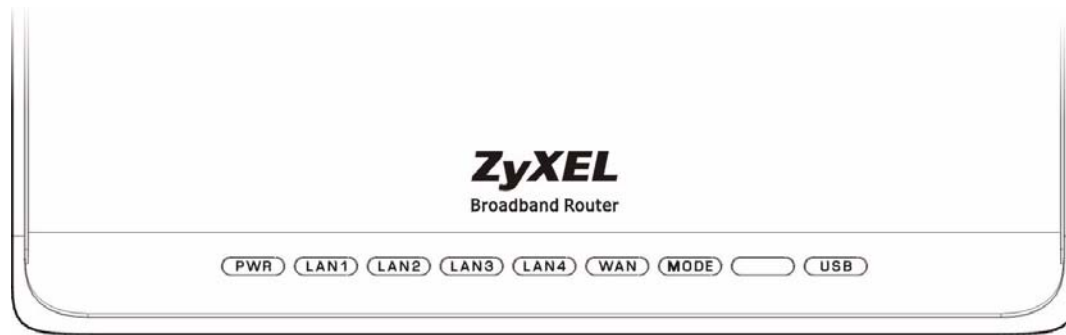
1.2 Good Habits for Managing Your ZyXEL Device

Here are some things you should do regularly.

- Change your password.
- Back up your configuration (and make sure you know how to reload it).
- Check www.zyxel.com for firmware upgrades.

1.3 Front Panel LEDs

Figure 3 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is performing testing.
	Red	On	Power to the ZyXEL Device is too low.
	None	Off	The ZyXEL Device is not receiving power.
LAN 1-4	Green	On	The ZyXEL Device has a successful 10Mb Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
	Amber	On	The ZyXEL Device has a successful 100Mb Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
	None	Off	The LAN is not connected.
WAN	Green	On	The ZyXEL Device has a successful 10Mb WAN connection.
		Blinking	The ZyXEL Device is sending/receiving data.
	Amber	On	The ZyXEL Device has a successful 100Mb Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
	None	Off	The WAN connection is not ready, or has failed.
P R	Amber	On	The ZyXEL Device is in print server mode.
	None	Off	The ZyXEL Device is in router mode.
USB		Off	The print server connection is not ready, or has failed.
	Green	On	The print server has a successful connection.
		Blinking	The print server is sending/receiving data.

CHAPTER 2

Introducing the Web Configurator

This chapter describes how to access the ZyXEL Device web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyXEL Device setup and management via 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.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

- 1 Make sure your ZyXEL Device hardware is properly connected and prepare your computer/computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 4 Change Password Screen

ZyXEL

Please enter a new password

Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess.

The administrator password should must be between 1 - 30 characters.

New Password:

Retype to Confirm:

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

2.3 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”.

2.3.1 Procedure to Use the Reset Button

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

2.4 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen. The screen varies depending on the operating mode you choose.

2.4.1 Router Mode Status

The following screen displays when the ZyXEL Device is set to router mode. The ZyXEL Device is in router mode by default.

Figure 5 Web Configurator Status Screen (Router Mode)

The screenshot shows the ZyXEL web configurator interface. The top bar includes the ZyXEL logo, a language dropdown set to 'English', and several utility icons. The left sidebar contains a tree view with categories: Network (WAN, LAN, DHCP Server, NAT, DDNS), Security (Firewall, Content Filter), Management (Static Route, Bandwidth MGMT, Remote MGMT, UPnP, Print Server), and Maintenance. The main content area is titled 'Status' and includes a 'Refresh Interval' dropdown (set to 'None') and a 'Refresh Now' button. The 'Device Information' section shows system details for 'P-335Plus' with firmware V3.60(AMD.0) | 07/24/2006. It lists WAN and LAN information including MAC addresses, IP addresses, subnets, and DHCP roles. The 'System Status' section shows the system is up for 1:17:27 on 2000-1-1/1:17:24, with 4.43% CPU usage and 23% memory usage. System settings like Firewall, Bandwidth Management, and UPnP are listed as enabled or disabled. The 'Interface Status' table shows both WAN and LAN interfaces are 'Up' at '100M/Full' rates. The 'Summary' section provides links for 'BW MGMT Monitor (Details...)', 'DHCP Table (Details...)', and 'Packet Statistics (Details...)'. The bottom of the screen features a 'Refresh Interval' dropdown set to 'None' and a 'Refresh Now' button.

The following table describes the icons shown in the **Status** screen.

Table 2 Status Screen Icon Key

ICON	DESCRIPTION
	Select a language from the drop-down list box to have the web configurator display in that language.
	Click this icon to open a web help page relevant to the screen you are currently configuring.
	Click this icon to open the setup wizard. The ZyXEL Device has a connection wizard and a bandwidth management wizard.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the web configurator.
	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.

The following table describes the labels shown in the **Status** screen.

Table 3 Web Configurator Status Screen (Router Mode)

LABEL	DESCRIPTION
Device Information	
System Name	This is the System Name you enter in the Maintenance > System > General screen. It is for identification purposes.
Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- DHCP	This shows the WAN port's DHCP role - Client or None .
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - Server, Relay or None .
System Status	
System Uptime	This is the total time the ZyXEL Device has been on.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
System Resource	
- CPU Usage	This number shows how many kilobytes of the heap memory the ZyXEL Device is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall. The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
- Memory Usage	This number shows the ZyXEL Device's total heap memory (in kilobytes). The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
System Setting	
- Firewall	This shows whether the firewall is active or not.
- Bandwidth Management	This shows whether the bandwidth management is active or not.
- UPnP	This shows whether UPnP is active or not.
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (Advanced) or not (Basic).
- System Operation Mode	This shows whether the ZyXEL Device is working as a router or a print server.
Interface Status	
Interface	This displays the ZyXEL Device port types.
Status	For the LAN and WAN ports, this field displays Down (line is down) or Up (line is up or connected).

Table 3 Web Configurator Status Screen (Router Mode) (continued)

LABEL	DESCRIPTION
Rate	For the LAN ports, this displays the port speed and duplex setting or N/A when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays N/A when the line is disconnected.
Summary	
BW MGNT Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
DHCP Table	Use this screen to view current DHCP client information.
Packet Statistics	Use this screen to view port status and packet specific statistics.

2.4.2 Print Server Mode Status

The following screen displays when the ZyXEL Device is set to print server mode.

Figure 6 Web Configurator Status Screen (Print Server Mode)







The screenshot displays the ZyXEL Web Configurator interface in Print Server Mode. The left sidebar shows the navigation menu with 'Print Server' selected. The main content area is titled 'Status' and includes a 'Refresh Interval' dropdown set to 'None' and a 'Refresh Now' button. The status is divided into three sections:

- Device Information:**
 - System Name: P-335Plus
 - Firmware Version: V3.60(AMD.0) | 07/24/2006
 - LAN Information:
 - MAC Address: 00:13:49:03:21:88
 - IP Address: 192.168.1.1
 - IP Subnet Mask: 255.255.255.0
- System Status:**
 - System Up Time: 1:31:05
 - Current Date/Time: 2000-1-1/1:31:2
 - System Resource:
 - CPU Usage: 1.50%
 - Memory Usage: 23%
 - System Setting:
 - Configuration Mode: Advanced
 - System Operation Mode: Print Server
- Interface Status:**

Interface	Status	Rate
LAN	Up	100M/Full

The following table describes the icons shown in the **Status** screen.

Table 4 Status Screen Icon Key

	DESCRIPTION
	Select a language from the drop-down list box to have the web configurator display in that language.
	Click this icon to open a web help page relevant to the screen you are currently configuring.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the web configurator.
	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.

The following table describes the labels shown in the **Status** screen.

Table 5 Web Configurator Status Screen (Print Server Mode)

LABEL	DESCRIPTION
Device Information	
System Name	This is the System Name you enter in the Maintenance > System > General screen. It is for identification purposes.
Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
System Status	
System Uptime	This is the total time the ZyXEL Device has been on.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
System Resource	
- CPU Usage	This number shows how many kilobytes of the heap memory the ZyXEL Device is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall. The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
- Memory Usage	This number shows the ZyXEL Device's total heap memory (in kilobytes). The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.

Table 5 Web Configurator Status Screen (Print Server Mode) (continued)

LABEL	DESCRIPTION
System Setting	
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (Advanced) or not (Basic).
- System Operation Mode	This shows whether the ZyXEL Device is working as a router or a print server.
Interface Status	
Interface	This displays the ZyXEL Device port types.
Status	This field displays Down (line is down) or Up (line is up or connected).
Rate	This displays the port speed and duplex setting or N/A when the line is disconnected.

2.4.3 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure ZyXEL Device features.

The following table lists the features available for each operating mode.

Table 6 Router and Print Server Mode Features Comparison

FEATURE	ROUTER MODE	PRINT SERVER MODE
Connection Wizard	O	
Banwidth Management Monitor	O	
DHCP Table	O	
Packet Statistics	O	
WAN	O	
LAN	O	O
DHCP Server	O	
NAT	O	
DDNS	O	
Firewall	O	
Content Filter	O	
Static Route	O	
Bandwidth Management	O	
Remote Management	O	
UPnP	O	
Print Server	O	O
Logs	O	O
Configuration Mode	O	O

Table Key: An O in a mode's column shows that the device mode has the specified feature. The information in this table was correct at the time of writing, although it may be subject to change.

The following table describes the sub-menus.

Table 7 Screens Summary

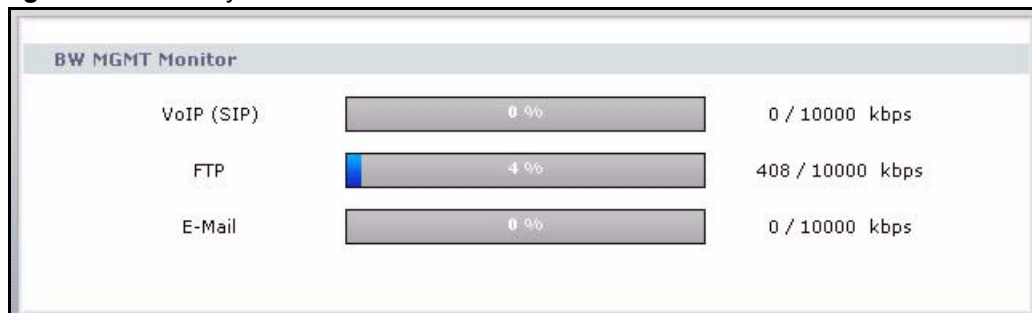
LINK	TAB	FUNCTION
Status		This screen shows the ZyXEL Device's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment and the WAN MAC address.
	Advanced	Use this screen to configure DNS servers and other advanced properties.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Advanced	Use this screen to enable other advanced properties.
DHCP Server	General	Use this screen to enable the ZyXEL Device's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the ZyXEL Device.
	Advanced	Use this screen to change your ZyXEL Device's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Filter	Use this screen to block certain web features and sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the ZyXEL Device to perform content filtering.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes.
Bandwidth MGMT	General	Use this screen to enable bandwidth management.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
	Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.

Table 7 Screens Summary

LINK	TAB	FUNCTION
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
UPnP	General	Use this screen to enable UPnP on the ZyXEL Device.
Print Server	Print Server	Use this screen to view the printer model name and to monitor the printer status.
Maintenance		
System	General	This screen contains administrative.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your ZyXEL Device's log settings.
Tools	Firmware	Use this screen to upload firmware to your ZyXEL Device.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your ZyXEL Device.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Config Mode	General	This screen allows you to display or hide the advanced screens or features.

2.4.4 Summary: Bandwidth Management Monitor

Select the **BW MGMT Monitor (Details...)** hyperlink in **Status** screen. View the bandwidth usage of the WAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 7 Summary: BW MGMT Monitor

2.4.5 Summary: DHCP Table

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 DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click the **DHCP Table (Details...)** hyperlink in the **Status** screen. 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 ZyXEL Device's DHCP server.

Figure 8 Summary: DHCP Table

DHCP Table			
#	IP Address	Host Name	MAC Address
1	192.168.1.33	tw11477-02	00:50:8d:48:59:1f

Refresh

The following table describes the labels in this screen.

Table 8 Summary: DHCP Table

	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the Host Name field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click Refresh to renew the screen.

2.4.6 Summary: Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** 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 9 Summary: Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	286	1345	0	0	384	0:08:13
LAN	100M/Full	1472	1543	0	0	0	0:09:37

System Up Time : 0:09:43

Poll Interval(s) : sec

The following table describes the labels in this screen.

Table 9 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the ZyXEL Device's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or Down when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays Down when the line is disconnected.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyXEL Device has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval(s) field.
Stop	Click Stop to stop refreshing statistics, click Stop .

CHAPTER 3

Connection Wizard

This chapter provides information on the wizard setup screens in the web configurator.

3.1 Wizard Setup

The web configurator's wizard setup helps you configure your device to access the Internet. Refer to your ISP (Internet Service Provider) checklist in the Quick Start Guide to know what to enter in each field. Leave a field blank if you don't have that information.

Note: The wizard is not available when the ZyXEL Device is in print server mode.

- 1 After you access the ZyXEL Device web configurator, click the **Go to Wizard setup** hyperlink.

You can click the **Go to Basic setup** or **Go to Advanced setup** hyperlink to skip this wizard setup and configure basic or advanced features accordingly.

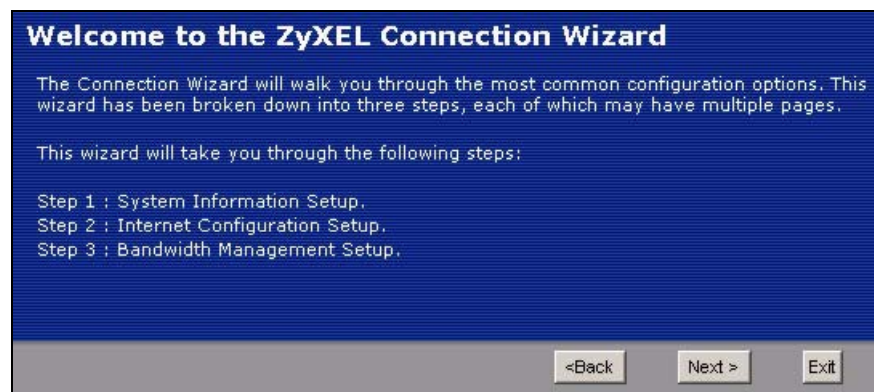
Figure 10 Select Wizard or Advanced Mode



- 2 Choose your language from the drop-down list box.
- 3 Click the **Next** button to proceed to the next screen.

Figure 11 Select a Language

4 Read the on-screen information and click **Next**.

Figure 12 Welcome to the Connection Wizard

3.2 Connection Wizard: STEP 1: System Information

System Information contains administrative and system-related information.

3.2.1 System Name

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

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start, Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

3.2.2 Domain Name

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

Click **Next** to configure the ZyXEL Device for Internet access.

Figure 13 Wizard Step 1: System Information

The following table describes the labels in this screen.

Table 10 Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the ZyXEL Device in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

3.3 Connection Wizard: STEP 2: Internet Configuration

The ZyXEL Device offers three Internet connection types. They are **Ethernet**, **PPP over Ethernet** or **PPTP**. The wizard attempts to detect which WAN connection type you are using. If the wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

This wizard screen varies according to the connection type that you select.

Figure 14 Wizard Step 3: ISP Parameters.



The following table describes the labels in this screen,

Table 11 Wizard Step 2: ISP Parameters

CONNECTION TYPE	DESCRIPTION
Ethernet	Select the Ethernet option when the WAN port is used as a regular Ethernet.
PPPoE	Select the PPP over Ethernet option for a dial-up connection. If your ISP gave you a an IP address and/or subnet mask, then select PPTP .
PPTP	Select the PPTP option for a dial-up connection.

3.3.1 Ethernet Connection

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 15 Wizard Step 2: Ethernet Connection



3.3.2 PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

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

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

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

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

Refer to the appendix for more information on PPPoE.

Figure 16 Wizard Step 2: PPPoE Connection

The following table describes the labels in this screen.

Table 12 Wizard Step 2: PPPoE Connection

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Connection Type	Select the PPP over Ethernet option for a dial-up connection.
Service Name	Type the name of your service provider.

Table 12 Wizard Step 2: PPPoE Connection

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

3.3.3 PPTP Connection

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

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

Refer to the appendix for more information on PPTP.

Note: The ZyXEL Device supports one PPTP server connection at any given time.

Figure 17 Wizard Step 2: PPTP Connection

STEP 1 → STEP 2 → STEP 3

Internet Configuration

ISP Parameters for Internet Access

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: PPTP

User Name: _____

Password: _____

PPTP Configuration

Get automatically from ISP (Default)

Use fixed IP address

My IP Address: 0.0.0.0

My IP Subnet Mask: 0.0.0.0

Server IP Address: 0.0.0.0

Connection ID/Name: _____

<Back Next > Exit

The following table describes the fields in this screen

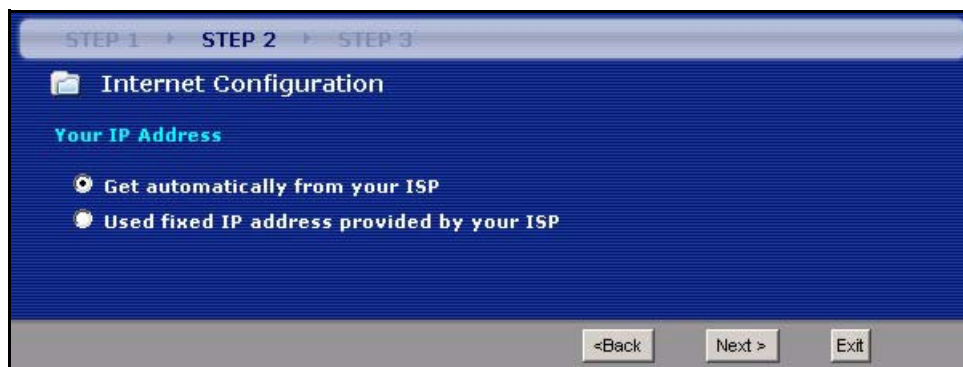
Table 13 Wizard Step 2: PPTP Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select PPTP from the drop-down list box. To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this radio button, provided by your ISP to give the ZyXEL Device a fixed, unique IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

3.3.4 Your IP Address

The following wizard screen allows you to assign a fixed IP address or give the ZyXEL Device an automatically assigned IP address depending on your ISP.

Figure 18 Wizard Step 2: Your IP Address



The following table describes the labels in this screen

Table 14 Wizard Step 2: Your IP Address

LABEL	DESCRIPTION
Get automatically from your ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection. If you choose this option, skip directly to section 3.3.9 .
Use fixed IP address provided by your ISP	Select this option if you were given IP address and/or DNS server settings by the ISP. The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

3.3.5 WAN IP Address Assignment

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

Table 15 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

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.

3.3.6 IP Address and Subnet Mask

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

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

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

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, 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.

3.3.7 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyXEL Device can get the DNS server addresses in the following ways.

- 1 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 **Wizard** and/or **WAN > Internet Connection** screen.
- 2 If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

3.3.8 WAN IP and DNS Server Address Assignment

The following wizard screen allows you to assign a fixed WAN IP address and DNS server addresses.

Figure 19 Wizard Step 2: WAN IP and DNS Server Addresses

STEP 1 → STEP 2 → STEP 3

Internet Configuration

WAN IP Address Assignment

My WAN IP Address: 172.23.23.49

My WAN IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

DNS Server Address Assignment

First DNS Server: 172.23.5.2

Second DNS Server: 172.23.5.1

Third DNS Server: 0.0.0.0

<Back Next > Exit

The following table describes the labels in this screen

Table 16 Wizard Step 2: WAN IP and DNS Server Addresses

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Enter your WAN IP address in this field. The WAN IP address should be in the same subnet as your DSL/Cable modem or router.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
System DNS Server Address Assignment (if applicable) 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 computer before you can access it. The ZyXEL Device uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.	
First DNS Server	Enter the DNS server's IP address in the fields provided.
Second DNS Server	If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.
Third DNS Server	
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

3.3.9 WAN MAC Address

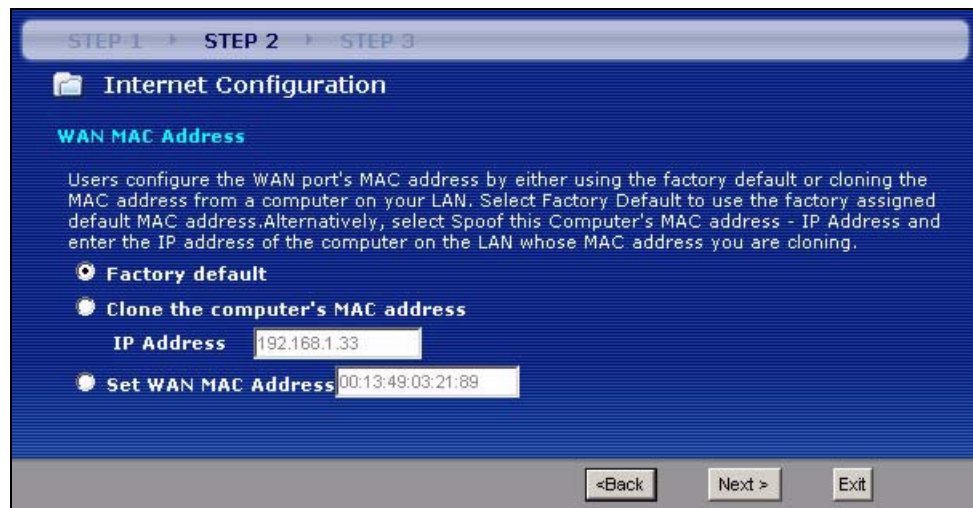
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Table 17 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(ZyXEL Device LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.

Figure 20 Wizard Step 2: WAN MAC Address



The following table describes the fields in this screen.

Table 18 Wizard Step 2: WAN MAC Address

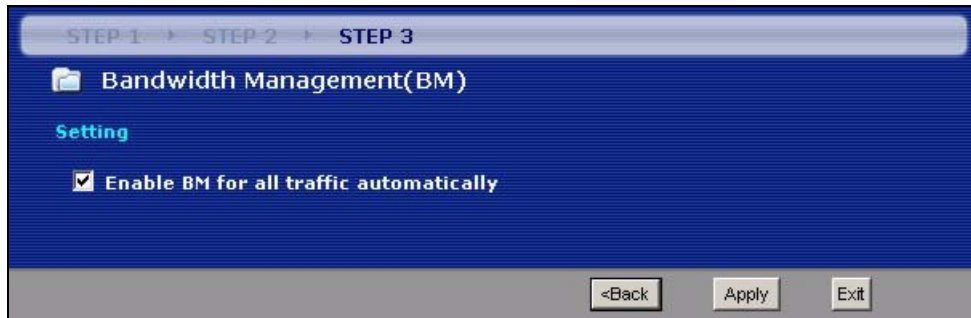
LABEL	DESCRIPTION
Factory Default	Select Factory Default to use the factory assigned default MAC address.
Clone the computer's MAC address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.

Table 18 Wizard Step 2: WAN MAC Address

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

3.4 Connection Wizard: STEP 3: Bandwidth management

Bandwidth management allows you to control the amount of bandwidth going out through the ZyXEL Device's WAN or LAN port and prioritize the distribution of the bandwidth according to the traffic type. This helps keep one service from using all of the available bandwidth and shutting out other users.

Figure 21 Wizard Step 3: Bandwidth Management

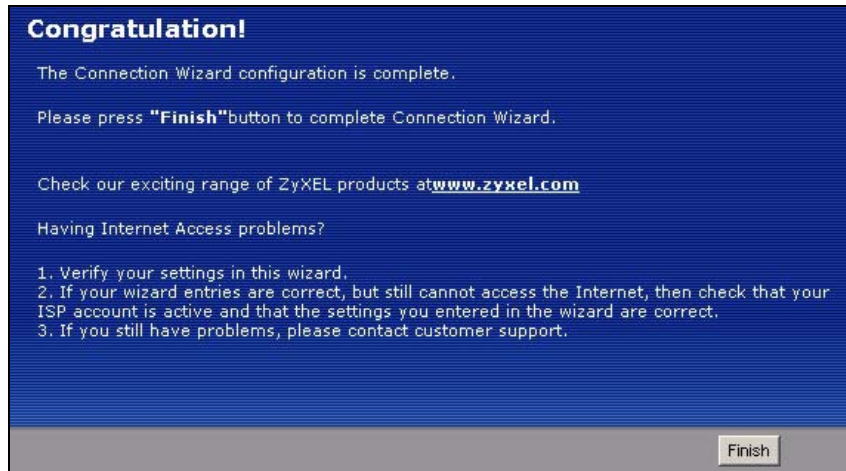
The following fields describe the label in this screen.

Table 19 Wizard Step 3: Bandwidth Management

LABEL	DESCRIPTION
Enable BM for all traffic automatically	Select the check box to have the ZyXEL Device apply bandwidth management to traffic going out through the ZyXEL Device's WAN or LAN port. Bandwidth is allocated according to the traffic type automatically. Real-time packets, such as VoIP traffic always get higher priority.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

3.5 Connection Wizard Complete

Follow the on-screen instructions and click **Finish** to complete the wizard setup.

Figure 22 Connection Wizard Complete

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

CHAPTER 4

WAN

This chapter describes how to configure WAN settings.

4.1 WAN Overview

See the chapter about the connection wizard for more information on the fields in the WAN screens.

4.2 WAN MAC Address

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

4.3 Internet Connection

To change your ZyXEL Device's Internet access settings, click **Network > WAN**. The screen differs by the encapsulation.

4.3.1 Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.

Figure 23 Ethernet Encapsulation

The screenshot shows the 'Internet Connection' window with the 'Advanced' tab selected. It is divided into several sections: 'ISP Parameters for Internet Access' with 'Encapsulation' set to 'Ethernet' and 'Service Type' set to 'Standard'; 'WAN IP Address Assignment' with the radio button 'Get automatically from ISP (Default)' selected; 'DNS Servers' with three entries, each set to 'From ISP' and having IP addresses 172.23.5.1, 172.23.5.2, and 0.0.0.0; and 'WAN MAC Address' with the radio button 'Factory default' selected. 'Apply' and 'Reset' buttons are at the bottom.

The following table describes the labels in this screen.

Table 20 Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from Standard , Telstra (RoadRunner Telstra authentication method), RR-Manager (Roadrunner Manager authentication method), RR-Toshiba (Roadrunner Toshiba authentication method) or Telia Login . The following fields do not appear with the Standard service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one. This field is not available for Telia Login .
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example login1.telia.com.
ReloginEvery(min) (Telia Login only)	The Telia server logs the ZyXEL Device out if the ZyXEL Device does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyXEL Device to wait between logins.
WAN IP Address Assignment	

Table 20 Ethernet Encapsulation

LABEL	DESCRIPTION
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
IP Subnet Mask	Enter the IP Subnet Mask in this field.
Gateway IP Address	Enter a Gateway IP Address (if your ISP gave you one) in this field.
DNS Servers	
First DNS Server	Select From ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Second DNS Server	
Third DNS Server	
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

4.3.2 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 **PPP over Ethernet** 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.

The screen shown next is for **PPPoE** encapsulation.

Figure 24 PPPoE Encapsulation

The screenshot displays the 'Advanced' configuration page for 'Internet Connection'. It is divided into several sections:

- ISP Parameters for Internet Access:**
 - Encapsulation: PPP over Ethernet (dropdown menu)
 - Service Name: (text input field) (optional)
 - User Name: (text input field)
 - Password: (password input field) [*****]
 - Retype to Confirm: (password input field) [*****]
 - Nailed-Up Connection
 - Idle Timeout (sec): 100 (in seconds)
- WAN IP Address Assignment:**
 - Get automatically from ISP (Default)
 - Use Fixed IP Address
 - My WAN IP Address: 0.0.0.0
 - Remote IP Address: 0.0.0.0
 - Remote IP Subnet Mask: 0.0.0.0
- DNS Servers:**
 - First DNS Server: From ISP (dropdown) | 172.23.5.2
 - Second DNS Server: From ISP (dropdown) | 172.23.5.1
 - Third DNS Server: From ISP (dropdown) | 0.0.0.0
- WAN MAC Address:**
 - Factory default
 - Clone the computer's MAC address - IP Address: 192.168.1.33
 - Set WAN MAC Address: 00:13:49:03:21:89

At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 21 PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPP over Ethernet choice is for a dial-up connection using PPPoE. The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
Remote IP Address	Enter the remote IP address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the remote IP subnet mask in this field.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select From ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the ZyXEL Device's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.

Table 21 PPPoE Encapsulation

LABEL	DESCRIPTION
Clone the computer's MAC address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

4.3.3 PPTP Encapsulation

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

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

The screen shown next is for **PPTP** encapsulation.

Figure 25 PPTP Encapsulation

Internet Connection **Advanced**

ISP Parameters for Internet Access

Encapsulation: PPTP

User Name: _____

Password: _____

Retype to Confirm: _____

Nailed-Up Connection

Idle Timeout (sec): 100 (in seconds)

PPTP Configuration

Get automatically from ISP (Default)

Use Fixed IP Address

My IP Address: 0.0.0.0

My IP Subnet Mask: 0.0.0.0

Server IP Address/Domain: 0.0.0.0

Connection ID/Name: _____

WAN IP Address Assignment

Get automatically from ISP (Default)

Use Fixed IP Address

My WAN IP Address: 0.0.0.0

Remote IP Address: 0.0.0.0

Remote IP Subnet Mask: 0.0.0.0

DNS Servers

First DNS Server: From ISP 172.23.5.2

Second DNS Server: From ISP 172.23.5.1

Third DNS Server: From ISP 0.0.0.0

WAN MAC Address

Factory default

Clone the computer's MAC address - IP Address: 192.168.1.33

Set WAN MAC Address: 00:13:49:03:21:89

.....

Apply Reset

The following table describes the labels in this screen.

Table 22 PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyXEL Device supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyXEL Device automatically disconnects from the PPTP server.
PPTP Configuration	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
Remote IP Address	Enter the remote IP address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the remote IP subnet mask in this field.
DNS Servers	

Table 22 PPTP Encapsulation

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select From ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

4.4 Advanced WAN Screen

To change your ZyXEL Device's advanced WAN settings, click **Network > WAN > Advanced**. The screen appears as shown.

Figure 26 Advanced

The screenshot shows the 'Advanced' configuration page for the Internet Connection. It features a 'Multicast Setup' section with a 'Multicast' dropdown menu currently set to 'None'. Below this is the 'Windows Networking (NetBIDS over TCP/IP)' section, which contains two unchecked checkboxes: 'Allow between LAN and WAN' and 'Allow Trigger Dial'. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 23 Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Select IGMP V-1 or IGMP V-2 or None . 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.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 5

LAN

This chapter describes how to configure LAN settings.

5.1 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

5.1.1 IP Pool Setup

The ZyXEL Device is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyXEL Device itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

5.1.2 System DNS Servers

Refer to the IP Address and Subnet Mask section in the **Connection Wizard** chapter.

5.2 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.

5.2.1 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.

5.2.2 IP Address and Subnet Mask

Refer to the IP Address and Subnet Mask section in the **Connection Wizard** chapter for this information.

5.2.3 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.

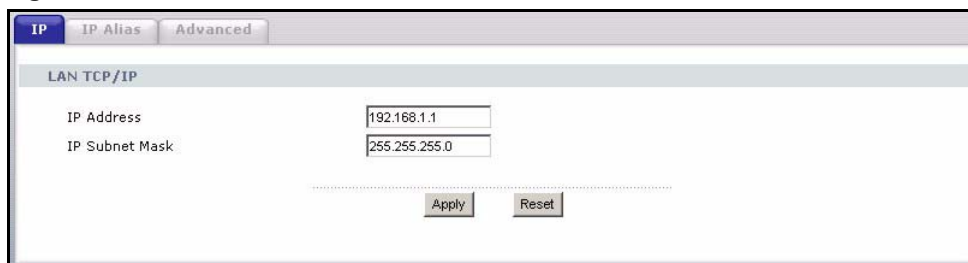
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed 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.

5.3 LAN IP Screen

Click **Network > LAN** to open the **IP** screen.

Figure 27 LAN IP



The screenshot displays the 'LAN TCP/IP' configuration page. At the top, there are three tabs: 'IP' (selected), 'IP Alias', and 'Advanced'. Below the tabs, the page title is 'LAN TCP/IP'. There are two input fields: 'IP Address' with the value '192.168.1.1' and 'IP Subnet Mask' with the value '255.255.255.0'. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 24 LAN IP

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your ZyXEL Device in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device 255.255.255.0.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

5.4 LAN IP Alias

IP Alias allows you to partition a physical network into different 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.

To change your ZyXEL Device's IP alias settings, click **Network > LAN > IP Alias**. The screen appears as shown.

Figure 28 LAN IP Alias

The screenshot shows the 'IP Alias' configuration page. At the top, there are tabs for 'IP', 'IP Alias', and 'Advanced'. The 'IP Alias' tab is selected. Below the tabs, there are two sections for configuring IP aliases. Each section starts with a checkbox labeled 'IP Alias 1' and 'IP Alias 2'. Below each checkbox are two input fields: 'IP Address' and 'IP Subnet Mask'. Both fields in both sections are currently set to '0.0.0.0'. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

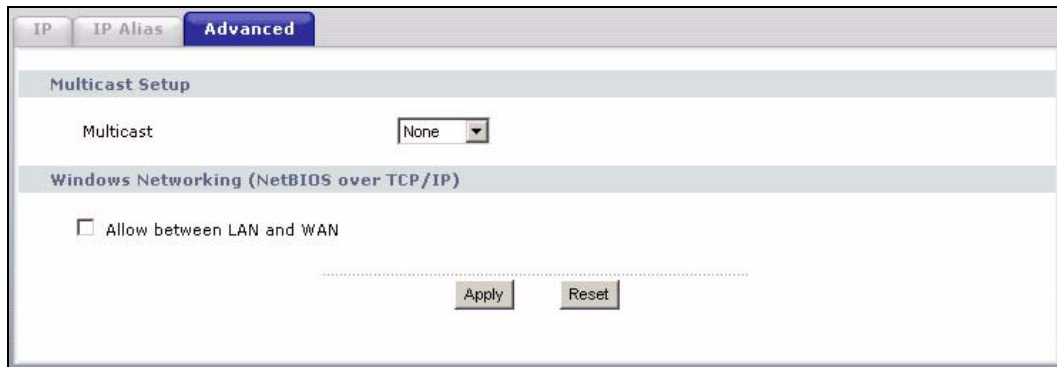
Table 25 LAN IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

5.5 Advanced LAN Screen

To change your ZyXEL Device's advanced IP settings, click **Network > LAN > Advanced**. The screen appears as shown.

Figure 29 Advanced LAN



The following table describes the labels in this screen.

Table 26 Advanced LAN

LABEL	DESCRIPTION
Multicast	Select IGMP V-1 or IGMP V-2 or None . 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.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	

Table 26 Advanced LAN

LABEL	DESCRIPTION
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 6

DHCP Server

6.1 DHCP

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 DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

6.2 DHCP Server General Screen

Click **Network > DHCP Server**. The following screen displays.

Figure 30 DHCP Server General

The following table describes the labels in this screen.

Table 27 DHCP Server General

LABEL	DESCRIPTION
Enable DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the Enable DHCP Server check box selected unless your ISP instructs you to do otherwise. Clear it to disable the ZyXEL Device acting as a DHCP server. When configured as a server, the ZyXEL Device provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.

Table 27 DHCP Server General

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

6.3 DHCP Server Advanced Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP clients.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your ZyXEL Device's static DHCP settings, click **Network > DHCP Server > Advanced**. The following screen displays.

Figure 31 DHCP Server Advanced

The screenshot shows the DHCP Server Advanced configuration interface. It features three tabs: 'General', 'Advanced' (which is active), and 'Client List'. The main content area is divided into two sections: 'Static DHCP Table' and 'DNS Server'.

Static DHCP Table: This section contains a table with 8 rows. The columns are '#', 'MAC Address', and 'IP Address'. All entries in the table are currently set to 00:00:00:00:00:00 for the MAC address and 0.0.0.0 for the IP address.

DNS Server: This section is titled 'DNS Servers Assigned by DHCP Server'. It includes three rows for configuring DNS servers:

- First DNS Server: From ISP (dropdown), 172.23.5.1 (input field)
- Second DNS Server: From ISP (dropdown), 172.23.5.2 (input field)
- Third DNS Server: From ISP (dropdown), 0.0.0.0 (input field)

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 28 DHCP Server Advanced

LABEL	DESCRIPTION
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
<p>DNS Servers Assigned by DHCP Server</p> <p>The ZyXEL Device passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The ZyXEL Device only passes this information to the LAN DHCP clients when you select the Enable DHCP Server check box. When you clear the Enable DHCP Server check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.</p>	
First DNS Server Second DNS Server Third DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select DNS Relay to have the ZyXEL Device act as a DNS proxy. The ZyXEL Device's LAN IP address displays in the field to the right (read-only). The ZyXEL Device tells the DHCP clients on the LAN that the ZyXEL Device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the ZyXEL Device's system DNS server (configured in the WAN > Internet Connection screen) and relays the response back to the computer. You can only select DNS Relay for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

6.4 Client List Screen

The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyXEL Device's DHCP server.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network > DHCP Server > Client List**.

Note: You can also view a read-only client list by clicking the **DHCP Table (Details...)** hyperlink in the **Status** screen.

The following screen displays.

Figure 32 Client List

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	tw	00:00:e8:7c:14:80	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 29 Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select this check box to have the ZyXEL Device always assign this IP address to this MAC address (and host name). After you click Apply , the MAC address and IP address also display in the Advanced screen (where you can edit them).
Refresh	Click Refresh to reload the DHCP table.

CHAPTER 7

Network Address Translation (NAT)

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 is changed to a different IP address known within another network.

7.2 Using NAT

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device.

7.2.1 Port Forwarding: Services and Port Numbers

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

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. 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.

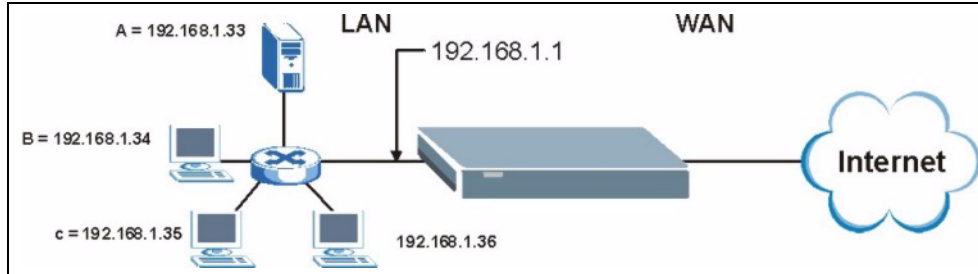
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Note: 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.

7.2.2 Configuring Servers Behind Port Forwarding (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

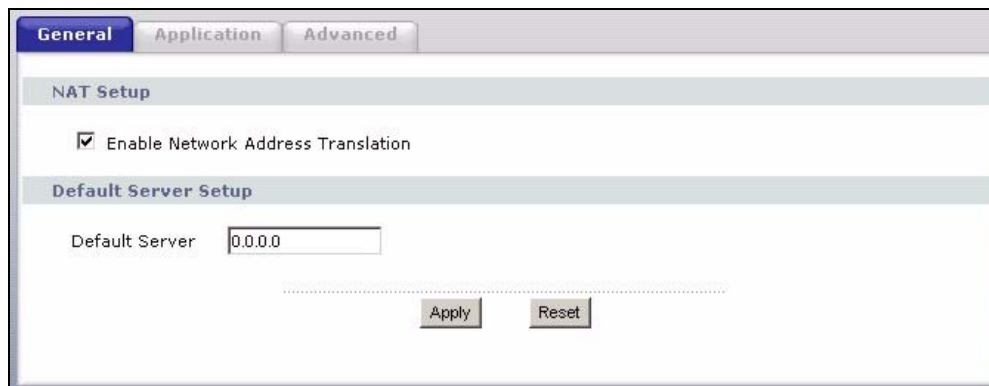
Figure 33 Multiple Servers Behind NAT Example



7.3 General NAT Screen

Click **Network > NAT** to open the **General** screen.

Figure 34 NAT General



The following table describes the labels in this screen.

Table 30 NAT General

LABEL	DESCRIPTION
Network Address Translation	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). Select the check box to enable NAT.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the Application screen. If you do not assign a Default Server IP address, the ZyXEL Device discards all packets received for ports that are not specified in the Application screen or remote management.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

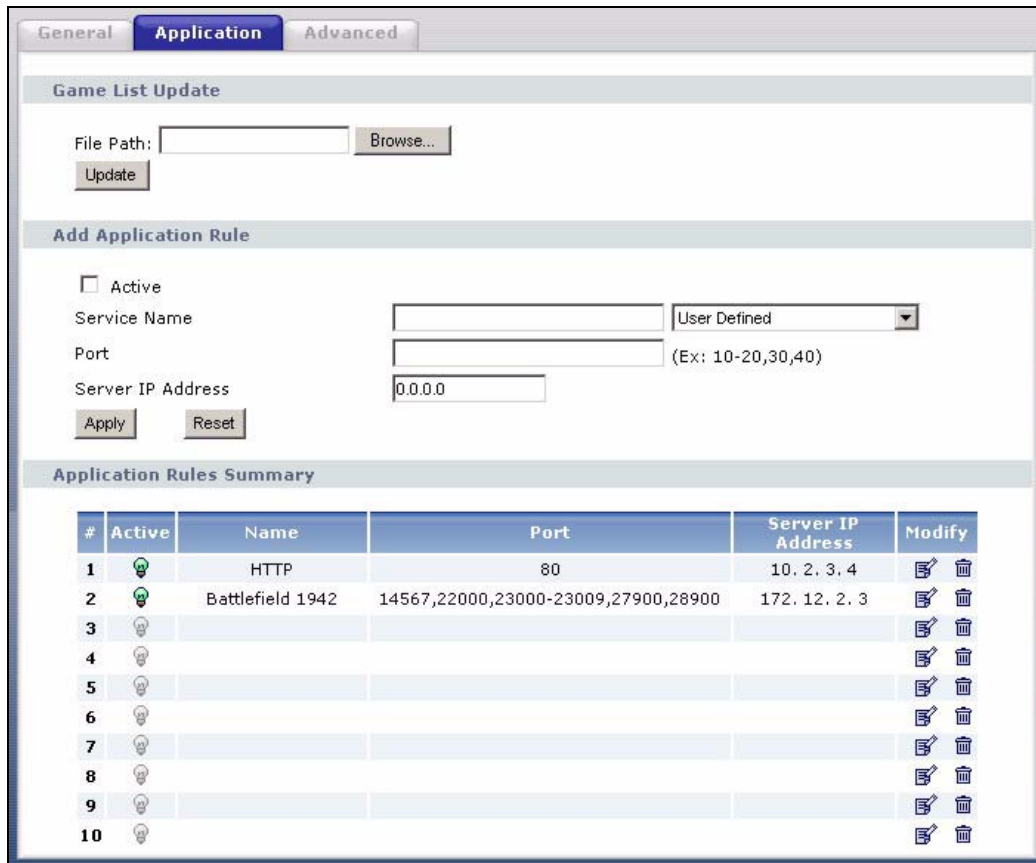
7.4 NAT Application Screen

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your ZyXEL Device's port forwarding settings, click **Network > NAT > Application**. The screen appears as shown.

Note: If you do not assign a **Default Server** IP address in the **NAT > General** screen, the ZyXEL Device discards all packets received for ports that are not specified in this screen or remote management.

Refer to [Appendix H on page 223](#) for port numbers commonly used for particular services.

Figure 35 NAT Application



The following table describes the labels in this screen.

Table 31 NAT Application

LABEL	DESCRIPTION
Game List Update	A game list includes the pre-defined service name(s) and port number(s). You can edit and upload it to the ZyXEL Device to replace the existing entries in the second field next to Service Name .
File Path	Type in the location of the file you want to upload in this field or click Browse... to find it.
Browse...	Click Browse... to find the.txt file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Update	Click Update to begin the upload process. This process may take up to two minutes.
Add Application Rule	
Active	Select the check box to enable this rule and the requested service can be forwarded to the host with a specified internal IP address. Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.

Table 31 NAT Application (continued)

LABEL	DESCRIPTION
Service Name	Type a name (of up to 31 printable characters) to identify this rule in the first field next to Service Name . Otherwise, select a predefined service in the second field next to Service Name . The predefined service name and port number(s) will display in the Service Name and Port fields.
Port	Type a port number(s) to be forwarded. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20. To specify two or more non-consecutive port numbers, separate them by a comma without spaces, such as 123,567.
Server IP Address	Type the inside IP address of the server that receives packets from the port(s) specified in the Port field.
Apply	Click Apply to save your changes to the Application Rules Summary table.
Reset	Click Reset to not save and return your new changes in the Service Name and Port fields to the previous one.
Application Rules Summary	
#	This is the number of an individual port forwarding server entry.
Active	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the Edit icon to display and modify an existing rule setting in the fields under Add Application Rule . Click the Remove icon to delete a rule.

7.4.1 Game List Example

Here is an example game list text file. The index number, service name and associated port(s) are specified by semi-colons (no spaces). Use the name=xxx (where xxx is the service name) to create a new service. Port range can be separated with a hyphen (-) (no spaces). Multiple (non-consecutive) ports can be separated by commas.

Figure 36 Game List Example

```
version=1
1;name=Battlefield 1942;port=14567,22000,23000-23009,27900,28900
2;name=Call of Duty;port=28960
3;name=Civilization IV;port=2056
4;name=Diablo I and II;port=6112-6119,4000
5;name=Doom 3;port=27666
6;name=F.E.A.R;port=27888
7;name=Final Fantasy XI;port=25,80,110,443,50000-65535
8;name=Guild Wars;port=6112,80
9;name=Half Life;port=6003,7002,27005,27010,27011,27015
10;name=Jedi Knight III: Jedi Academy;port=28060-28062,28070-28081
11;name=Need for Speed: Hot Pursuit 2;port=1230,8511-
8512,27900,28900,61200-61230
12;name=Neverwinter Nights;port=5120-5300,6500,27900,28900
13;name=Quake 2;port=27910
14;name=Quake 3;port=27660,27960
15;name=Rainbow Six 3: Raven Shield;port=7777-7787,8777-8787
16;name=Serious Sam II;port=25600-25605
17;name=Silent Hunter III;port=17997-18003
18;name=Soldier of Fortune II;port=20100-20112
19;name=Starcraft;port=6112-6119,4000
20;name=Star Trek: Elite Force II;port=29250,29256
21;name=SWAT 4;port=10480-10483
22;name=Warcraft II and III;port=6112-6119,4000
23;name=World of Warcraft;port=3724
```

7.5 Trigger Port Forwarding

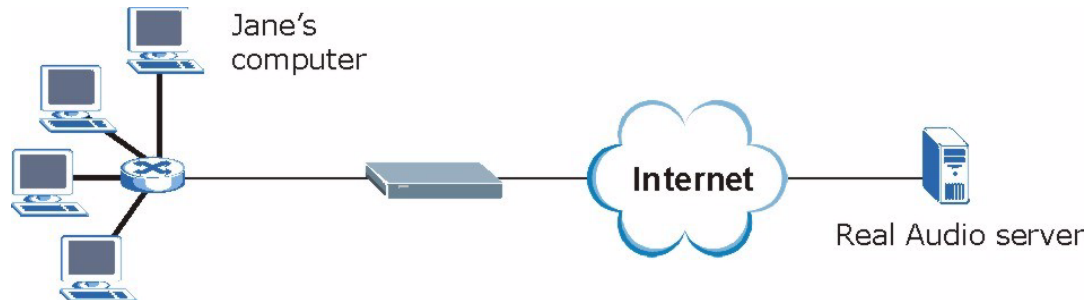
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyXEL Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyXEL Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

7.5.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 37 Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a “trigger” port and causes the ZyXEL Device to record Jane’s computer IP address. The ZyXEL Device associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The ZyXEL Device forwards the traffic to Jane’s computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyXEL Device times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

7.5.2 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is going coming from inside the ZyXEL Device and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

7.6 NAT Advanced Screen

To change your ZyXEL Device’s trigger port settings, click **Network > NAT > Advanced**. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 38 NAT Advanced

The following table describes the labels in this screen.

Table 32 NAT Advanced

LABEL	DESCRIPTION
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create. When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyXEL Device. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.

Table 32 NAT Advanced

LABEL	DESCRIPTION
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 8

Dynamic DNS

8.1 Dynamic DNS Introduction

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. 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 and still reach your hostname.

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

8.2 Dynamic DNS Screen

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

Figure 39 Dynamic DNS

The following table describes the labels in this screen.

Table 33 Dynamic DNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when CustomDNS is selected in the DDNS Type field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 9

Firewall

This chapter gives some background information on firewalls and explains how to get started with the ZyXEL Device firewall.

9.1 Introduction to Firewall

9.1.1 What is a Firewall?

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

9.1.2 Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

9.1.3 About the ZyXEL Device Firewall

The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The ZyXEL Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The ZyXEL Device is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyXEL Device has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

9.1.4 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via web configurator.
- 2 Think about access control before you connect to the network in any way, including attaching a modem to the port.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

9.2 Triangle Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the ZyXEL Device's LAN IP address, return traffic may not go through the ZyXEL Device. This is called an asymmetrical or "triangle" route. This causes the ZyXEL Device to reset the connection, as the connection has not been acknowledged.

You can have the ZyXEL Device permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyXEL Device. A better solution is to use IP alias to put the ZyXEL Device and the backup gateway on separate subnets.

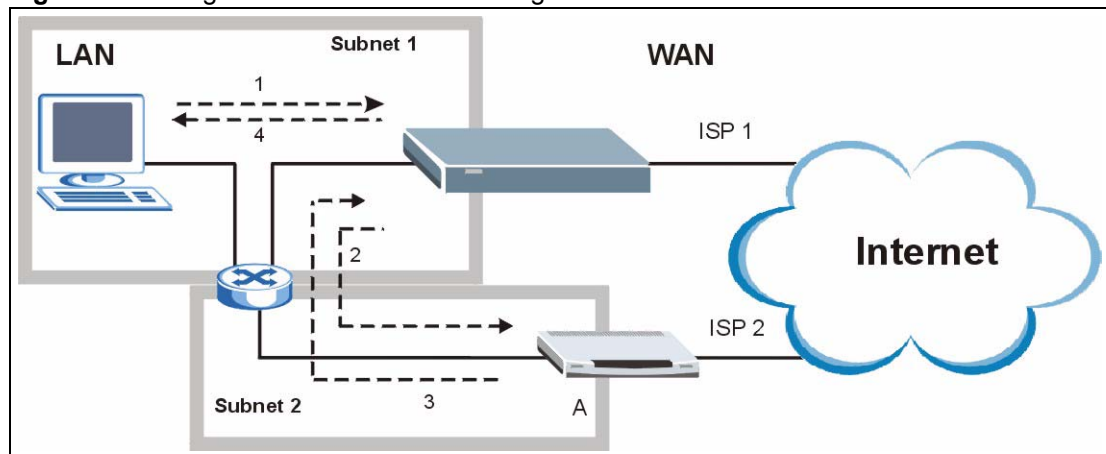
9.2.1 Triangle Routes and IP Alias

You can use IP alias instead of allowing triangle routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway A in different subnets, all returning network traffic must pass through the ZyXEL Device to your LAN. The following steps describe such a scenario.

- 1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2 The ZyXEL Device reroutes the packet to Gateway A, which is in **Subnet 2**.
- 3 The reply from the WAN goes to the ZyXEL Device.
- 4 The ZyXEL Device then sends it to the computer on the LAN in **Subnet 1**.

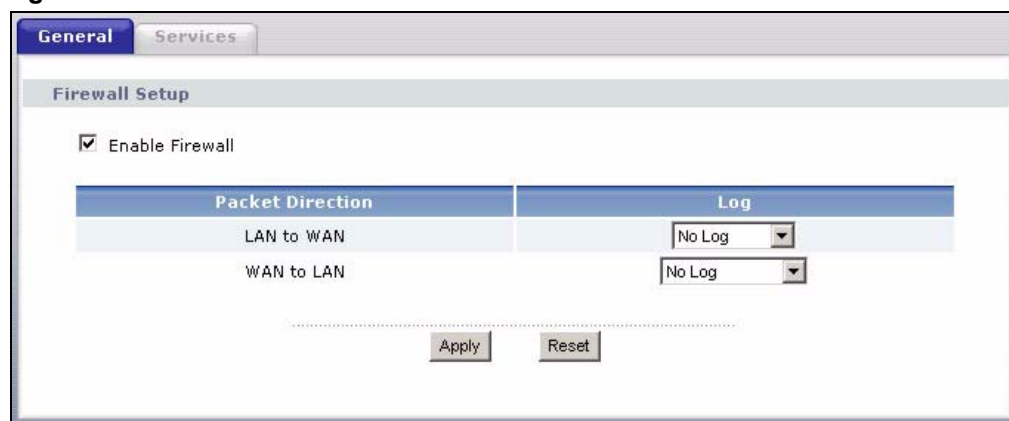
Figure 40 Using IP Alias to Solve the Triangle Route Problem



9.3 General Firewall Screen

Click **Security > Firewall** to open the **General** screen.

Figure 41 General



The following table describes the labels in this screen.

Table 34 Firewall General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Packet Direction	This is the direction of travel of packets. Firewall rules are grouped based on the direction of travel of packets to which they apply.
Log	Select whether to create a log for packets that are traveling in the selected direction when the packets are blocked or forwarded. To log packets related to firewall rules, make sure that Access Control under Log is selected in the Logs > Log Settings screen.
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen again.

9.4 Services Screen

Click **Security > Firewall > Services**. The screen appears as shown next.

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Figure 42 Services

General Services

ICMP

Respond to Ping on

Do not respond to requests for unauthorized services

Service Setup

Enable Services Blocking

Available Services

- Custom Port...
- Any(TCP)
- Any(UDP)
- IPSEC_TUNNEL(ESP:0)
- MULTICAST(IGMP:0)
- PING(ICMP:0)
- PPTP_TUNNEL(GRE:0)
- MSN Messenger

Blocked Services

Select "Custom Port", you can give new port range for blocking

Type Port Number ~

Schedule to Block

Day to Block

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Block (24-Hour Format)

All day

From : Start (hour) (min) End (hour) (min)

Misc setting

Bypass Triangle Route

Max NAT/Firewall Session Per User:

The following table describes the labels in this screen.

Table 35 Firewall Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN & WAN to reply to both incoming LAN and WAN Ping requests.

Table 35 Firewall Services

LABEL	DESCRIPTION
Do not respond to requests for unauthorized services	<p>Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. By default this option is not selected and the ZyXEL Device will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports.</p> <p>Note that the probing packets must first traverse the ZyXEL Device's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyXEL Device reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.</p>
Enable Services Blocking	Select this check box to enable this feature.
Available Services	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click Add to add the port to the Blocked Services field.
Blocked Services	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking.
Custom Port	A custom port is a service that is not available in the pre-defined Available Services list and you must define using the next two fields.
Type	Choose the IP port (TCP or UDP) that defines your customized port from the drop down list box.
Port Number	Enter the port number range that defines the service. For example, if you want to define the Gnutella service, then select TCP type and enter a port range from 6345 to 6349.
Add	Select a service from the Available Services drop-down list and then click Add to add a service to the Blocked Services
Delete	Select a service from the Blocked Services list and then click Delete to remove this service from the list.
Clear All	Click Clear All to empty the Blocked Services .
Day to Block:	Select a check box to configure which days of the week (or everyday) you want service blocking to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting All Day . You can also configure specific times by selecting From and entering the start time in the Start (hour) and Start (min) fields and the end time in the End (hour) and End (min) fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Bypass Triangle Route	Select this check box to have the ZyXEL Device firewall ignore the use of triangle route topology on the network.
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen again.

CHAPTER 10

Content Filtering

This chapter provides a brief overview of content filtering using the embedded web GUI.

10.1 Introduction to Content Filtering

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords.

10.2 Restrict Web Features

The ZyXEL Device can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

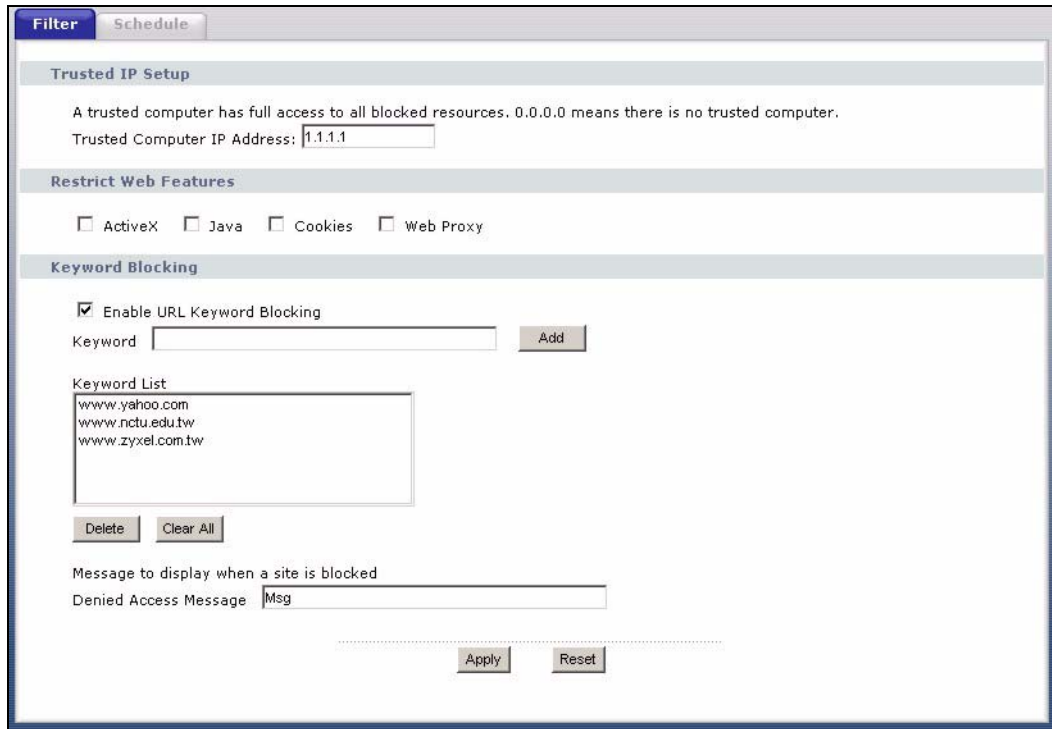
10.3 Days and Times

The ZyXEL Device also allows you to define time periods and days during which the ZyXEL Device performs content filtering.

10.4 Filter Screen

Click **Security > Content Filter** to open the **Filter** screen.

Figure 43 Content Filter: Filter



The following table describes the labels in this screen.

Table 36 Content Filter: Filter

LABEL	DESCRIPTION
Trusted Computer IP Address	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The ZyXEL Device can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.

Table 36 Content Filter: Filter

LABEL	DESCRIPTION
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click Add after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click Delete to remove it. The keyword disappears from the text box after you click Apply .
Clear All	Click this button to remove all of the listed keywords.
Message to display when a site is blocked.	
Denied Access Message	Enter a message to be displayed when a user tries to access a restricted web site. The default message is Please contact your network administrator!!
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh

10.5 Schedule

Click **Security > Content Filter > Schedule**. The following screen displays.

Figure 44 Content Filter: Schedule

The screenshot shows a web interface for configuring a content filter schedule. At the top, there are two tabs: 'Filter' and 'Schedule', with 'Schedule' selected. Below the tabs is a section titled 'Schedule to Block'. Under this section, there are two main configuration areas:

- Day to Block:** This area has a checked radio button for 'Everyday' and seven unchecked checkboxes for 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'.
- Time of Day to Block (24-Hour Format):** This area has a selected radio button for 'All day' and an unselected radio button for 'From:'. The 'From:' option includes two sets of input fields: 'Start' with '0' in the hour field and '0' in the minute field, and 'End' with '0' in the hour field and '0' in the minute field.

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 37 Content Filter: Schedule

LABEL	DESCRIPTION
Day to Block	Select check boxes for the days that you want the ZyXEL Device to perform content filtering. Select the Everyday check box to have content filtering turned on all days of the week.
Time of Day to Block (24-Hour Format)	Time of Day to Block allows the administrator to define during which time periods content filtering is enabled. Time of Day to Block restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. Select All Day to have content filtering always active on the days selected in Day to Block with time of day limitations not enforced. Select From and enter the time period, in 24-hour format, during which content filtering will be enforced.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh

10.6 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

10.6.1 Domain Name or IP Address URL Checking

By default, the ZyXEL Device checks the URL's domain name or IP address when performing keyword blocking.

This means that the ZyXEL Device checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

10.6.2 Full Path URL Checking

Full path URL checking has the ZyXEL Device check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

10.6.3 File Name URL Checking

Filename URL checking has the ZyXEL Device check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL

www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

CHAPTER 11

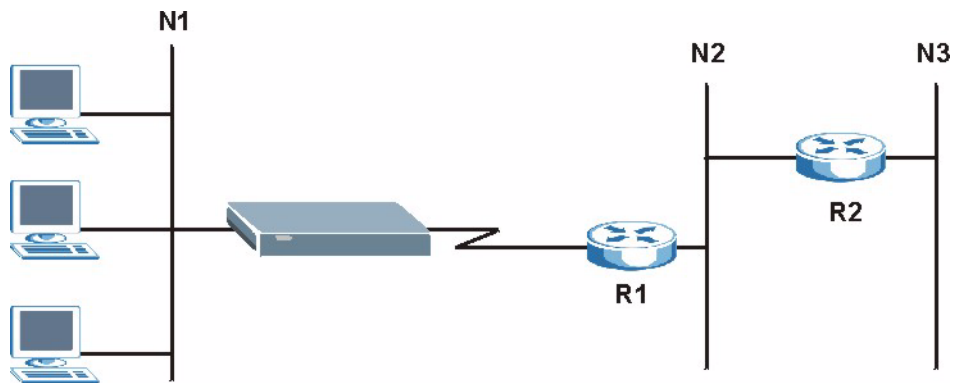
Static Route Screens

This chapter shows you how to configure static routes for your ZyXEL Device.

11.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network **N2** in the following figure through remote node router **R1**. However, the ZyXEL Device is unable to route a packet to network **N3** because it doesn't know that there is a route through the same remote node router **R1** (via gateway router **R2**). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

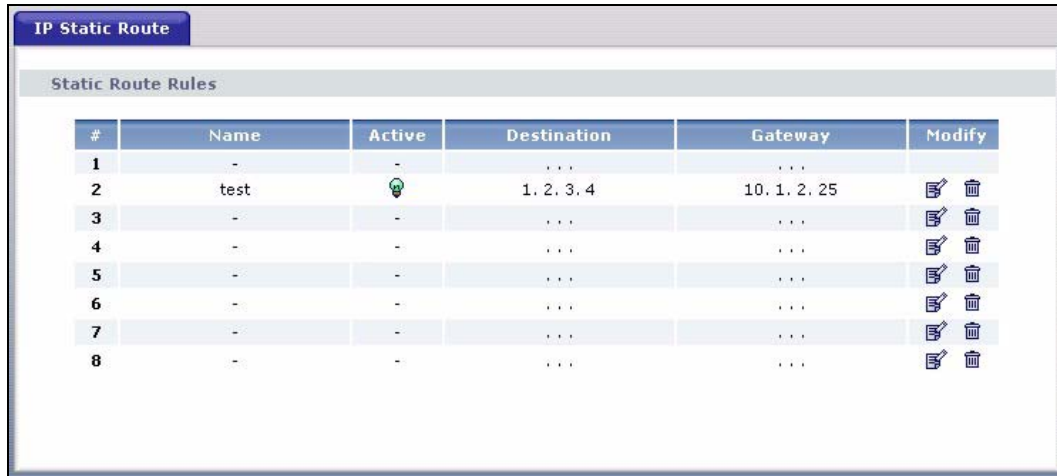
Figure 45 Example of Static Routing Topology



11.2 IP Static Route Screen

Click **Management > Static Route** to open the **IP Static Route** screen. The following screen displays.

Figure 46 IP Static Route



The screenshot shows the 'IP Static Route' screen with a table titled 'Static Route Rules'. The table has six columns: '#', 'Name', 'Active', 'Destination', 'Gateway', and 'Modify'. There are eight rows. Row 2 is highlighted and shows 'test' in the Name column, a green lightbulb icon in the Active column, '1. 2. 3. 4' in the Destination column, and '10. 1. 2. 25' in the Gateway column. The Modify column for row 2 contains an edit icon and a delete icon. All other rows have dashes in the Name and Active columns and ellipses in the Destination and Gateway columns.

#	Name	Active	Destination	Gateway	Modify
1	-	-	
2	test		1. 2. 3. 4	10. 1. 2. 25	
3	-	-	
4	-	-	
5	-	-	
6	-	-	
7	-	-	
8	-	-	

The following table describes the labels in this screen.

Table 38 IP Static Route

LABEL	DESCRIPTION
#	This is the index number of an individual static route. The first entry is for the default route and not editable.
Name	This is the name that describes or identifies this route.
Active	This icon is turned on when this static route is active. Click the Edit icon under Modify and select the Active checkbox in the Static Route Setup screen to enable the static route. Clear the checkbox to disable this static route without having to delete the entry.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the remote nodes.
Modify	Click the Edit icon to open the static route setup screen. Modify a static route or create a new static route in the Static Route Setup screen. Click the Remove icon to delete a static route.

11.2.1 Static Route Setup Screen

To edit a static route, click the edit icon under **Modify**. The following screen displays. Fill in the required information for each static route.

Figure 47 Static Route Setup

The following table describes the labels in this screen.

Table 39 Static Route Setup

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Private	This parameter determines if the ZyXEL Device will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previous screen and not save your changes.

CHAPTER 12

Bandwidth Management

This chapter contains information about configuring bandwidth management, editing rules and viewing the ZyXEL Device's bandwidth management logs.

12.1 Bandwidth Management Overview

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

The ZyXEL Device applies bandwidth management to traffic that it forwards out through an interface. The ZyXEL Device does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management.

- The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WAN to WAN / ZyXEL Device) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.
- The sum of the bandwidth allotments that apply to the LAN port (WAN to LAN, LAN to LAN / ZyXEL Device) must be less than or equal to 100,000 kbps (you cannot configure the bandwidth budget for the LAN port).

12.2 Application-based Bandwidth Management

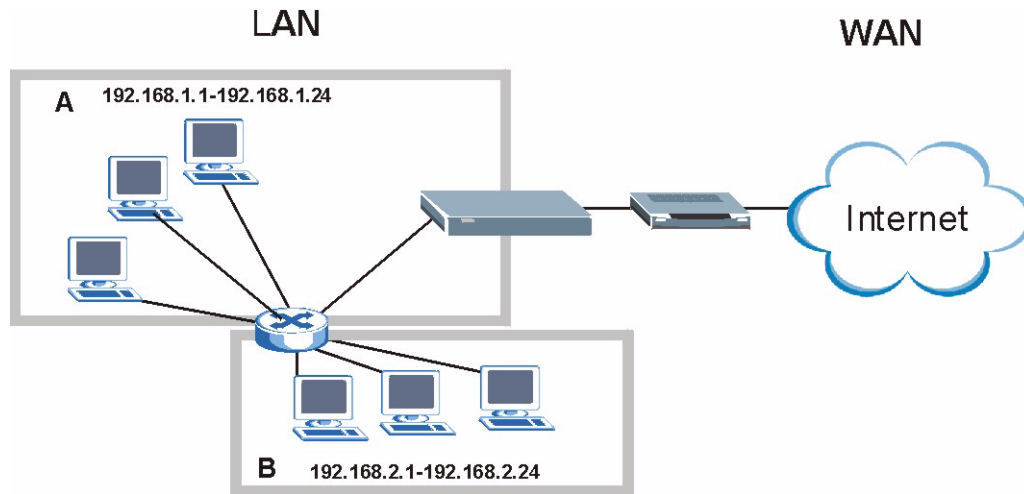
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

12.3 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet **A** and another for subnet **B**.

Figure 48 Subnet-based Bandwidth Management Example



12.4 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 40 Application and Subnet-based Bandwidth Management Example

	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

12.5 Bandwidth Management Priorities

The following table describes the priorities that you can apply to traffic that the ZyXEL Device forwards out through an interface.

Table 41 Bandwidth Management Priorities

PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED.	
High	Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).
Mid	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Low	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.

12.6 Predefined Bandwidth Management Services

The following is a description of the services that you can select and to which you can apply media bandwidth management using the wizard screens.

Table 42 Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
Xbox Live	This is Microsoft's online gaming service that lets you play multiplayer Xbox games on the Internet via broadband technology. Xbox Live uses port 3074.
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80
eMule	These programs use advanced file sharing applications relying on central servers to search for files. They use default port 4662.
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files using ports 6881 to 6889. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by corporation and trading, that is, the client downloads the file in small pieces and share the pieces with other peers to get other half of the file.

Table 42 Media Bandwidth Management Setup: Services (continued)

SERVICE	DESCRIPTION
MSN Webcam	MSN messenger allows you to chat online and send instant messages. If you use MSN messenger and also have a webcam, you can send your image/photo in real-time along with messages
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.

12.6.1 Services and Port Numbers

The commonly used services and port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the **DNS** service. **(UDP/TCP:53)** means UDP port 53 and TCP port 53.

Table 43 Commonly Used Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.

Table 43 Commonly Used Services

SERVICE	DESCRIPTION
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).

Table 43 Commonly Used Services

SERVICE	DESCRIPTION
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

12.7 Default Bandwidth Management Classes and Priorities

If you enable bandwidth management but do not configure a rule for critical traffic like VoIP, the voice traffic may then get delayed due to insufficient bandwidth. With the automatic traffic classifier feature activated, the ZyXEL Device automatically assigns a default bandwidth management class and priority to traffic that does not match any of the user-defined rules. The traffic is classified based on the traffic type. Real-time traffic always gets higher priority over other traffic.

The following table shows you the priorities between the three default classes (**AutoClass_H**, **AutoClass_M** and **Default Class**) and user-defined rules. 6 is the highest priority.

Table 44 Bandwidth Management Priority with Default Classes

CLASS TYPE	PRIORITY
User-defined with high priority	6
AutoClass_H	5
User-defined with medium priority	4
AutoClass_M	3
User-defined with low priority	2
Default Class	1

12.8 Bandwidth Management General Configuration

Click **Management > Bandwidth MGMT** to open the bandwidth management **General** screen.

Figure 49 Bandwidth Management: General



The following table describes the labels in this screen.

Table 45 Bandwidth Management: General

LABEL	DESCRIPTION
Enable Bandwidth Management	Select this check box to have the ZyXEL Device apply bandwidth management. Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.
Enable Automatic Traffic Classifier	This field is only applicable when you select the Enable Bandwidth Management check box. Select this check box to have the ZyXEL Device base on the default bandwidth classes to apply bandwidth management. Real-time packets, such as VoIP traffic always get higher priority.
Apply	Click Apply to save your customized settings.
Reset	Click Reset to begin configuring this screen afresh.

12.9 Bandwidth Management Advanced Configuration

Click **Management > Bandwidth MGMT > Advanced** to open the bandwidth management **Advanced** screen.

Figure 50 Bandwidth Management: Advanced

Management Bandwidth

Upstream Bandwidth (kbps)(10 kbps reserved)

Application List

#	Enable	Service	Priority	Advanced Setting
1	<input type="checkbox"/>	XBox Live	High	
2	<input type="checkbox"/>	VoIP (SIP)	High	
3	<input type="checkbox"/>	FTP	High	
4	<input type="checkbox"/>	E-Mail	High	
5	<input type="checkbox"/>	eMule/eDonkey	High	
6	<input type="checkbox"/>	BitTorrent	High	
7	<input type="checkbox"/>	MSN Webcam	High	
8	<input type="checkbox"/>	WWW	High	

User-defined Service

#	Enable	Direction	Service Name	Priority	Modify
1	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
2	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
3	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
4	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
5	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
6	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
7	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
8	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
9	<input type="checkbox"/>	To LAN	<input type="text"/>	High	
10	<input type="checkbox"/>	To LAN	<input type="text"/>	High	

The following table describes the labels in this screen.

Table 46 Bandwidth Management: Advanced

	DESCRIPTION
Upstream Bandwidth (kbps)	Enter the amount of bandwidth in kbps (2 to 100,000) that you want to allocate for traffic. 20 kbps to 20,000 kbps is recommended. The recommendation is to set this speed to be equal to or less than the speed of the broadband device connected to the WAN port. For example, set the speed to 1000 Kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1000 Kbps.
Application List	Use this table to allocate specific amounts of bandwidth based on the pre-defined service.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the ZyXEL Device apply this bandwidth management rule.
Service	This is the name of the service.
Priority	Select a priority from the drop down list box. Choose High , Mid or Low .
Advanced Setting	Click the Edit icon to open the Rule Configuration screen where you can modify the rule.
User-defined Service	Use this table to allocate specific amounts of bandwidth to specific applications and/or subnets.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the ZyXEL Device apply this bandwidth management rule.
Direction	Select To LAN to apply bandwidth management to traffic that the ZyXEL Device forwards to the LAN. Select To WAN to apply bandwidth management to traffic that the ZyXEL Device forwards to the WAN.
Service Name	Enter a descriptive name of up to 19 alphanumeric characters, including spaces.
Priority	Select a priority from the drop down list box. Choose High , Mid or Low .
Modify	Click the Edit icon to open the Rule Configuration screen. Modify an existing rule or create a new rule in the Rule Configuration screen. See Section 12.9.2 on page 115 for more information. Click the Remove icon to delete a rule.
Apply	Click Apply to save your customized settings.
Reset	Click Reset to begin configuring this screen afresh.

12.9.1 Rule Configuration with the Pre-defined Service

To edit a bandwidth management rule for the pre-defined service in the ZyXEL Device, click the **Edit** icon in the **Application List** table of the **Advanced** screen. The following screen displays.

Figure 51 Bandwidth Management Rule Configuration: Pre-defined Service

#	Enable	Direction	Bandwidth	Destination Port	Source Port	Protocol
1	<input type="checkbox"/>	LAN	Minimum Bandwidth 10 (kbps)	-	110	TCP
2	<input type="checkbox"/>	WAN	Minimum Bandwidth 10 (kbps)	25	-	TCP

OK Cancel

The following table describes the labels in this screen.

Table 47 Bandwidth Management Rule Configuration: Pre-defined Service

LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Enable	Select an interface's check box to enable bandwidth management on that interface.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management.
Bandwidth	Select Maximum Bandwidth or Minimum Bandwidth and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Port	This is the port number of the destination. See Table 43 on page 108 for some common services and port numbers.
Source Port	This is the port number of the source. See Table 43 on page 108 for some common services and port numbers.
Protocol	This is the protocol (TCP or UDP) used for the service.
OK	Click OK to save your customized settings.
Cancel	Click Cancel to exit this screen without saving.

12.9.2 Rule Configuration with the User-defined Service

In addition to the pre-defined services, if you want to edit a bandwidth management rule for other applications and/or subnets, click the **Edit** icon in the **User-defined Service** table of the **Advanced** screen. The following screen displays.

Figure 52 Bandwidth Management Rule Configuration: User-defined Service

The following table describes the labels in this screen.

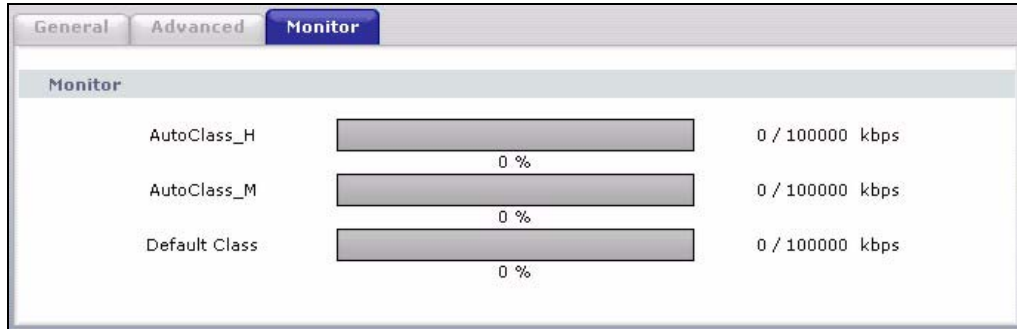
Table 48 Bandwidth Management Rule Configuration: User-defined Service

LABEL	DESCRIPTION
BW Budget	Select Maximum Bandwidth or Minimum Bandwidth and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a Destination Address . Refer to the appendices for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See Table 43 on page 108 for some common services and port numbers.
Source Address	Enter the source IP address in dotted decimal notation.
Source Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a Source Address . Refer to the appendices for more information on IP subnetting.
Source Port	Enter the port number of the source. See Table 43 on page 108 for some common services and port numbers.
Protocol	Select the protocol (TCP or UDP) or select User defined and enter the protocol (service type) number.
OK	Click OK to save your customized settings.
Cancel	Click Cancel to exit this screen without saving.

12.10 Bandwidth Management Monitor

Click **Management > Bandwidth MGMT > Monitor** to open the bandwidth management **Monitor** screen. View the bandwidth usage of the WAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 53 Bandwidth Management: Monitor



CHAPTER 13

Remote Management Screens

This chapter provides information on the Remote Management screens.

13.1 Remote Management Overview

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

Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

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

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

Note: When you choose **WAN** or **LAN & WAN**, you still need to configure a firewall rule to allow access.

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

13.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 You have disabled that service in one of the remote management screens.
- 2 The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.

- 3 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- 4 There is a firewall rule that blocks it.

13.1.2 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.

13.1.3 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. You can change the timeout period in the **System** screen

13.2 WWW Screen

To change your ZyXEL Device's World Wide Web settings, click **Management > Remote MGMT** to display the **WWW** screen.

Figure 54 WWW Remote Management

The screenshot shows the 'WWW' configuration page. At the top, there are navigation tabs: 'WWW', 'Telnet', 'FTP', and 'DNS'. Below the tabs, the 'WWW' section is active. It contains three main configuration items: 'Server Port' with a text box containing '80', 'Server Access' with a dropdown menu set to 'LAN', and 'Secured Client IP Address' with radio buttons for 'All' (selected) and 'Selected' (with a text box containing '0.0.0.0'). Below these is a 'Note' icon and text: '1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.' At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 49 WWW Remote Management

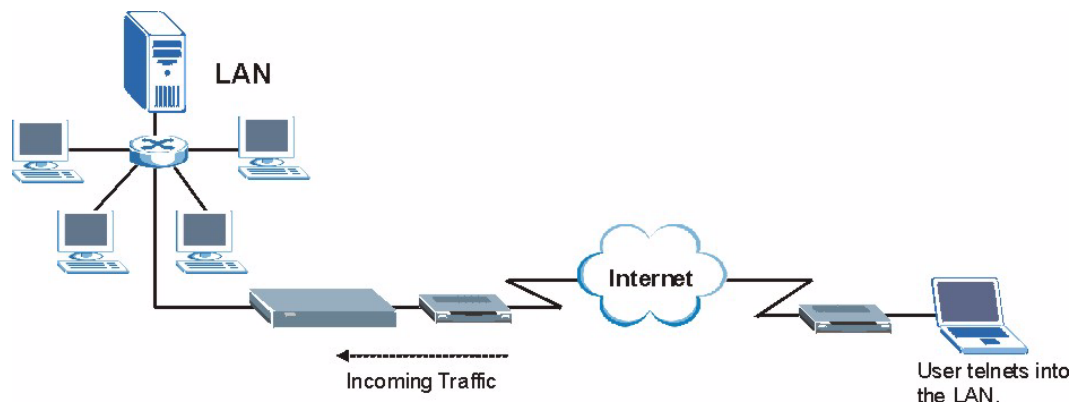
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.

Table 49 WWW Remote Management

LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select All to allow any computer to access the ZyXEL Device using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

13.3 Telnet

You can configure your ZyXEL Device for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the ZyXEL Device.

Figure 55 Telnet Configuration on a TCP/IP Network

13.4 Telnet Screen

To change your ZyXEL Device's Telnet settings, click **Management > Remote MGMT > Telnet**. The following screen displays.

Figure 56 Telnet Remote Management

The following table describes the labels in this screen.

Table 50 Telnet Remote Management

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

13.5 FTP Screen

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

To change your ZyXEL Device's FTP settings, click **Management > Remote MGMT > FTP**. The screen appears as shown.

Figure 57 FTP Remote Management

The following table describes the labels in this screen.

Table 51 FTP Remote Management

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

13.6 DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on Wizard Setup for background information.

To change your ZyXEL Device's DNS settings, click **Management > Remote MGMT > DNS**. The screen appears as shown.

Figure 58 DNS Remote Management

The following table describes the labels in this screen.

Table 52 DNS Remote Management

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the ZyXEL Device. Select All to allow any computer to send DNS queries to the ZyXEL Device. Choose Selected to just allow the computer with the IP address that you specify to send DNS queries to the ZyXEL Device.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 14

UPnP

This chapter introduces the Universal Plug and Play feature.

14.1 Universal Plug and Play Overview

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.

14.1.1 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.

14.1.2 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:

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

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

See the chapter on SUA/NAT for further information about NAT.

14.1.3 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.

14.2 UPnP and ZyXEL

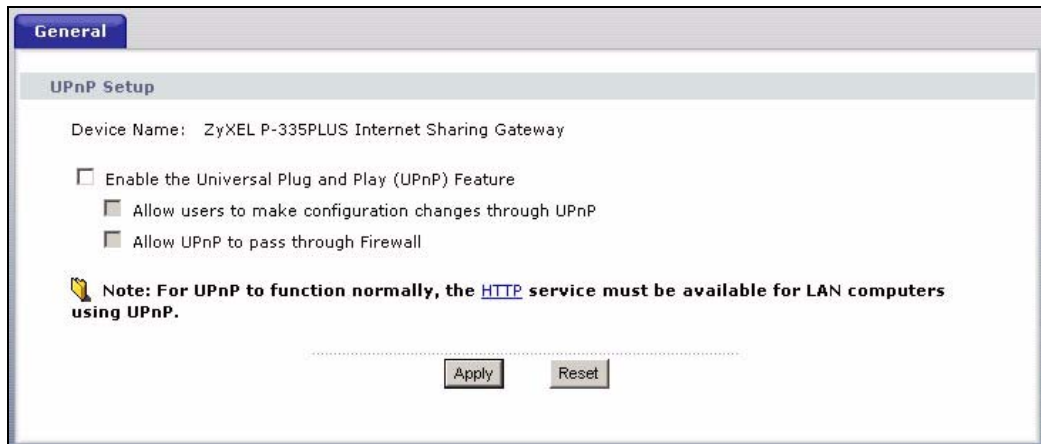
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

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

14.3 UPnP Screen

Click the **UPnP** link under **Management** to display the UPnP screen.

Figure 59 Configuring UPnP



The screenshot shows the 'UPnP Setup' configuration page within a 'General' tab. The page displays the device name as 'ZyXEL P-335PLUS Internet Sharing Gateway'. There are three checkboxes: 'Enable the Universal Plug and Play (UPnP) Feature' (unchecked), 'Allow users to make configuration changes through UPnP' (checked), and 'Allow UPnP to pass through Firewall' (checked). A note with a yellow warning icon states: 'Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.' At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 53 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) feature	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.
Allow UPnP to pass through Firewall	UPnP broadcasts are only allowed on the LAN. If you block LAN-to-LAN/ZyXEL Device traffic using the firewall, then you need to select this check box to allow UPnP-enabled traffic to pass through the firewall. This setting remains active until you disable UPnP. Clear this check box if you do not want to create a hole in the firewall for UPnP application packets (for example, MSN packets).
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

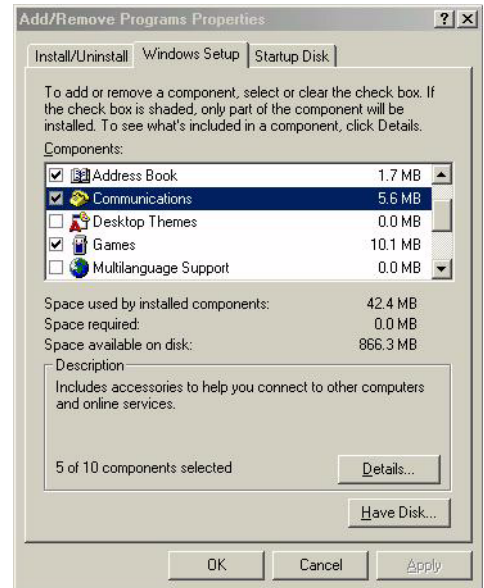
14.4 Installing UPnP in Windows Example

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

14.4.1 Installing UPnP in Windows Me

Follow the steps below to install 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**.



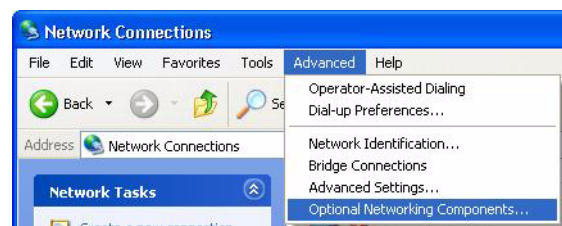
- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.



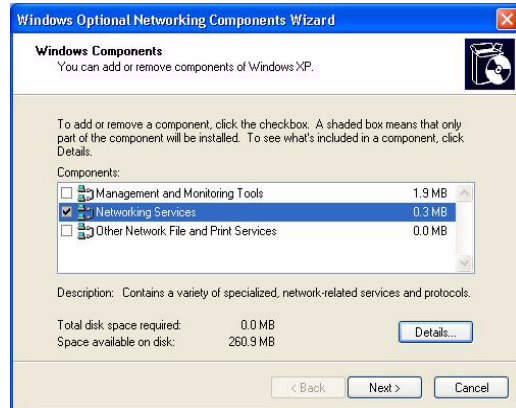
14.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

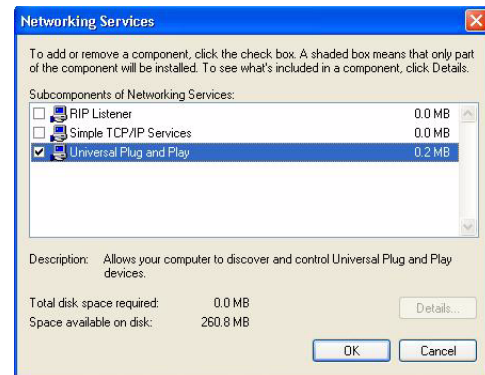
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**. The **Windows Optional Networking Components Wizard** window displays.



- 4 Select **Networking Service** in the **Components** selection box and click **Details**.



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.
- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



14.5 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.

14.5.1 Auto-discover Your UPnP-enabled Network Device

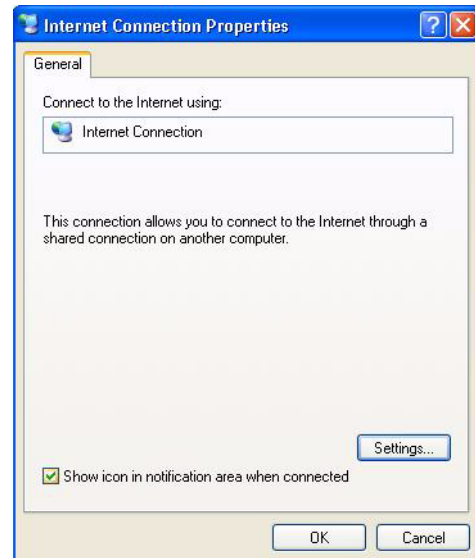
- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.



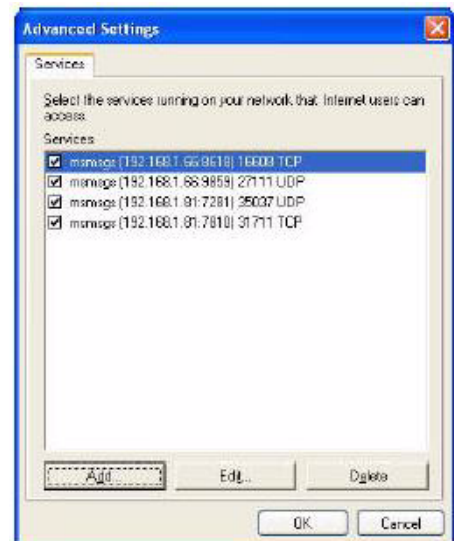
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.
- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 5 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray



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

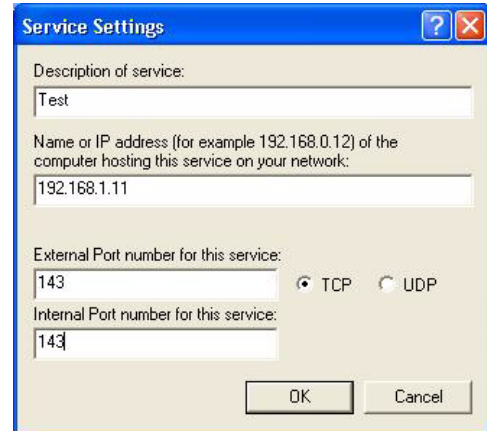


14.5.2 Web Configurator Easy Access

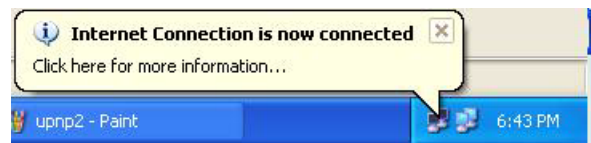
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

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**.



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.
- 6 Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.



14.5.3 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 is 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**.



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



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



CHAPTER 15

Print Server

This chapter discusses how to configure the print server on the ZyXEL Device.

15.1 Print Server Overview

A print server is a device or software that provides users on a network with shared access to one or more printers. The print server acts as a buffer, holding the information to be printed out in memory until the printer becomes free. Print servers can be programmed to print jobs in the order that they arrive or to give priority to particular users who, in effect, can jump the print queue. The advantages of a print server include efficient use of expensive resources, for example, laser printers. This avoids having to retry to print if the printer is initially busy.

15.2 ZyXEL Device Print Server

The ZyXEL Device has a built-in print server that allows the LAN to share a printer. There is no need to assign a dedicated computer as a print server or have a standalone print server device.

Print requests are sent by each computer to the ZyXEL Device. These request are placed in a queue and are then printed when the printer becomes available.

The print server driver must be set up on each computer in your network that you want to use the print server. Before you set up the print server driver, make sure the USB printer and your computer are connected to the ZyXEL Device and that both the ZyXEL Device, your computer and the USB printer are turned on.

Use [Chapter 16 on page 133](#) to set up your computer to use the ZyXEL Device print server driver.

15.3 Print Server Screen

Click the **Print Server** link under **Management** to display the **Print Server** screen.

Figure 60 Configuring Print Server

The screenshot shows a web-based configuration interface for a print server. At the top, there is a blue header with the text 'Print Server'. Below this is a light gray sub-header also labeled 'Print Server'. The main content area contains three rows of configuration data. The first row shows 'Print Device Name' followed by a text input field containing 'PrintServer'. The second row shows 'Print Model Name' followed by the text ':EPSON Stylus C43'. The third row shows 'Print Port Status' followed by the text ': Ready'. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset', separated by a dotted line.

The following table describes the labels in this screen.

Table 54 Configuring Print Server

LABEL	DESCRIPTION
Print Device Name	Type a Print Device Name (of up to 31 printable characters) for recognition of the associated printer on the print server network. This name is displayed on a computer on the print server network when a print job is executed.
Print Model Name	This displays the model name of the printer currently connected to the ZyXEL Device print server.
Print Port Status	This field displays the print server status on the ZyXEL Device. Ready: The print server has established a TCP/IP connection with a printer, is online and ready to print. Printing: A computer on the print server network is executed a print job. PaperOut: The printer loading tray has no paper to perform the printing job Offline: The computers in the print server network cannot use the print server. Make sure a USB v1.1 compliant printer is connected to the ZyXEL Device's USB port and powered on.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to configure the Print Device Name afresh.

CHAPTER 16

Print Server Driver Setup

This chapter shows you how to set up a print server driver for a Windows or Macintosh computer.

16.1 Installation Requirements

To install the print server driver you will need the following requirements

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X
- A computer with an Ethernet port
- An Ethernet cable and a USB cable

16.2 Windows 95/98 SE/Me/2000/XP/NT 4.0

We use the Windows 2000 screens here as an example. Screens and steps vary slightly for different Windows operating systems.

Note: You must have a printer with a driver and you need to know the IP address of the ZyXEL Device.

- 1 Insert the CD (supplied with the ZyXEL Device) into the CD-ROM driver on your computer. The CD Autorun screen is displayed.
- 2 Select **Network Print Server Setup**.

Figure 61 CD Autorun Screen



3 You can either

- use the **Setup Wizard for Windows NT/2000/XP** to install the print monitor and open the setup wizard automatically
- or
- use the **Setup Wizard for Windows 98/ME/NT/2000/XP** to install the print monitor in a specified file location and open the setup wizard (by running the PSWizard.exe file in the folder you selected) manually.

Figure 62 CD Autorun Screen: Printer Server Driver Setup



16.2.1 Print Server Driver Setup Wizard

After you install the print monitor and open the setup wizard, follow the steps below to install the print server driver on your computer.

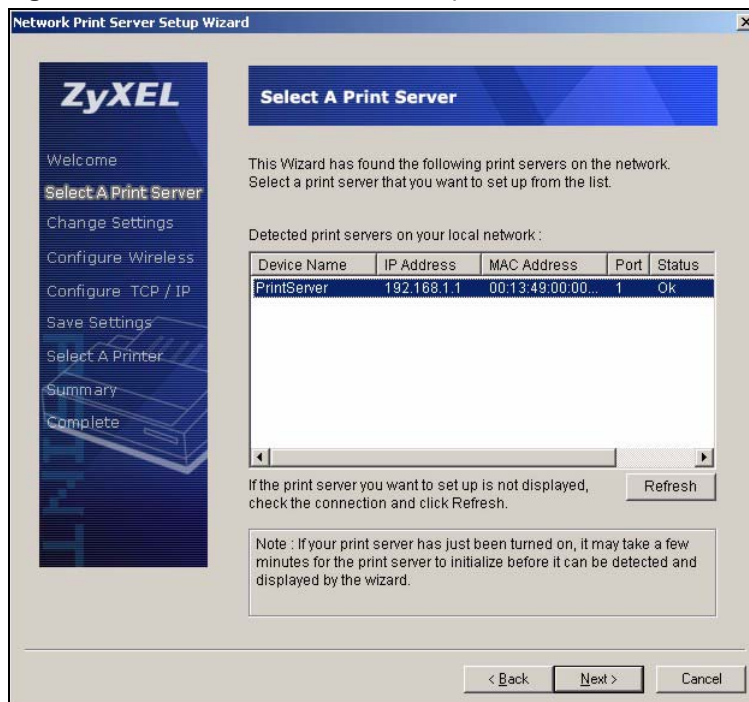
- 1 The **Welcome** screen displays. Click **Next** to continue.

Figure 63 Network Print Server Setup Wizard: Welcome



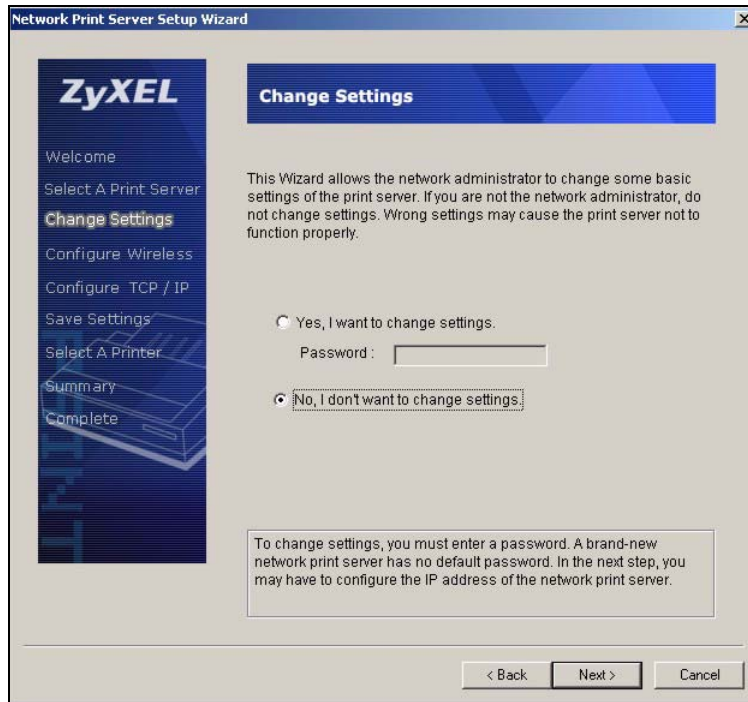
- 2 The **Select A Print Server** screen displays. The wizard automatically detects whether or not a print server is connected to your computer. Make sure that your ZyXEL Device is correctly connected and a compatible USB printer is connected to the ZyXEL Device. Highlight the print server and click **Next** to continue.

Figure 64 Network Print Server Setup Wizard: Select A Print Server



- The **Change Settings** screen displays. If you want to change your print server's IP address, select **Yes, I want to change settings**, leave the **Password** field blank and click **Next**. The print server's IP address is the ZyXEL Device's IP address. Since the wizard detects your print server's IP address automatically, it's recommended that you select **No, I don't want to change settings** and click **Next** to use the current print server settings and continue with the wizard.

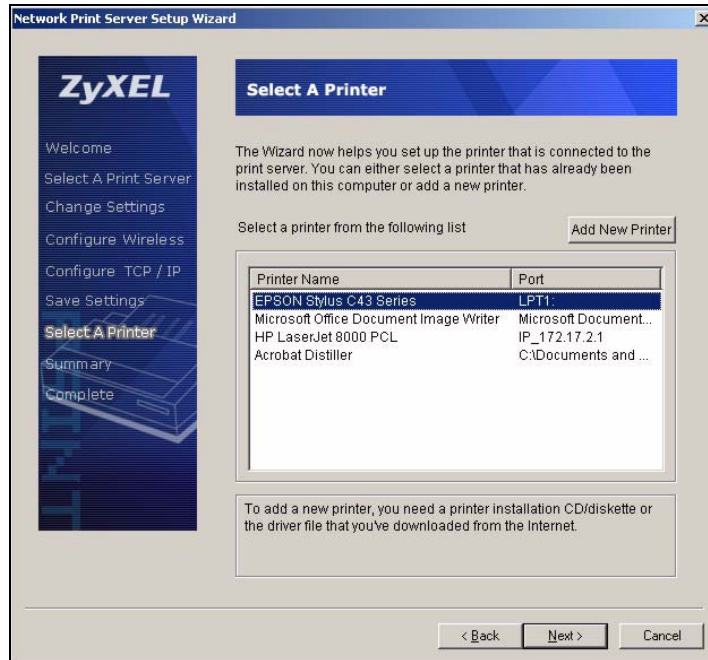
Figure 65 Network Print Server Setup Wizard: Change Settings



- 4 Select the USB printer that is connected to the ZyXEL Device if you have added it on your computer already and click **Next**.

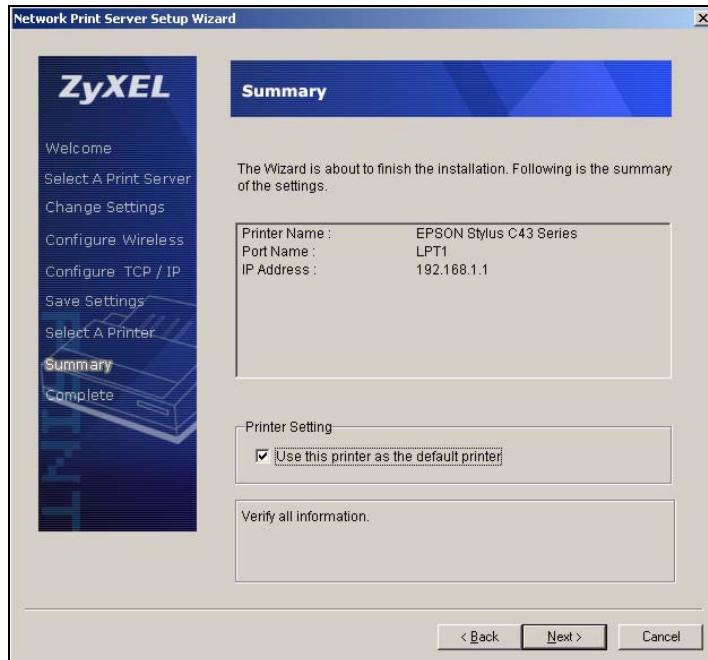
If your printer is not listed, click **Add New Printer** and see [Section 16.2.2 on page 139](#) for how to add a printer on your computer. After you have added a printer, the **Select A Printer** screen displays again. Select the printer you have added and click **Next** to continue.

Figure 66 Network Print Server Setup Wizard: Select A Printer



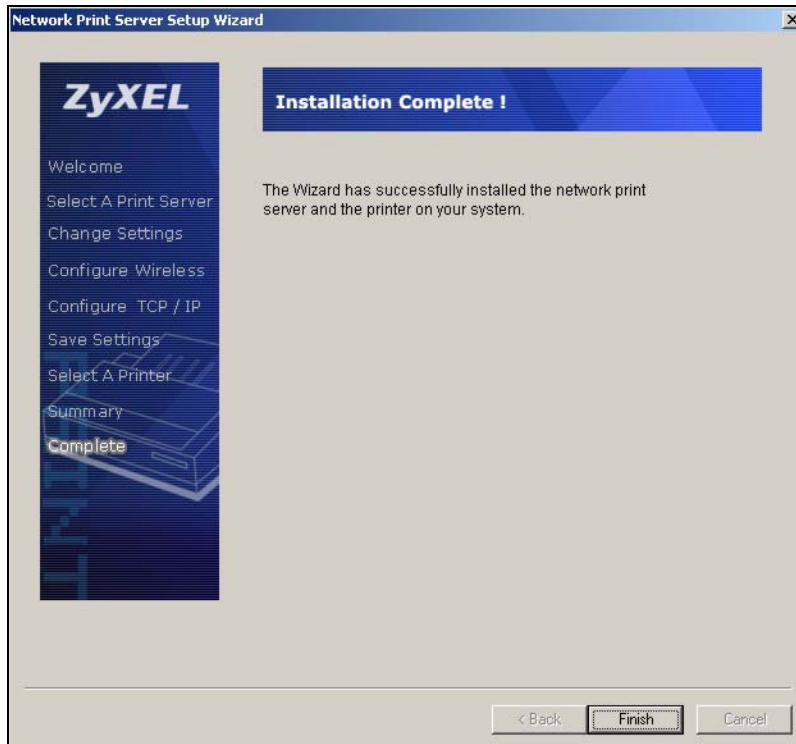
- 5 A **Summary** screen displays. Check your settings and click **Next** to continue.

Figure 67 Network Print Server Setup Wizard: Summary



- 6 Click **Finish** to save and close your **Network Print Server Setup Wizard**. Your print server driver setup is complete.

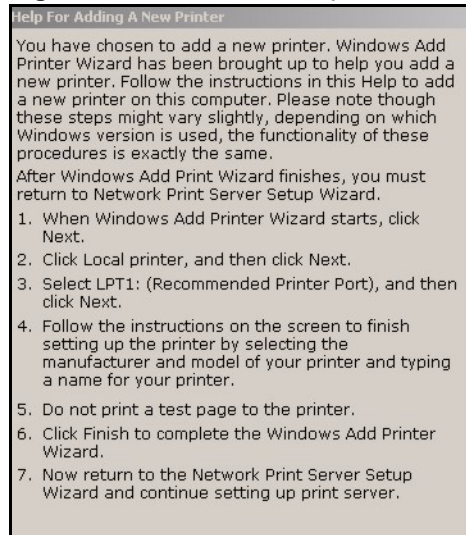
Figure 68 Network Print Server Setup Wizard: Installation Complete



16.2.2 Adding a New Printer

- 1 Click **Add New Printer** in the **Network Print Server Setup Wizard: Select A Printer** screen (see [Figure 66 on page 137](#)). A help dialog box pops up to guide you through the adding printer process.

Figure 69 Add Printer Help



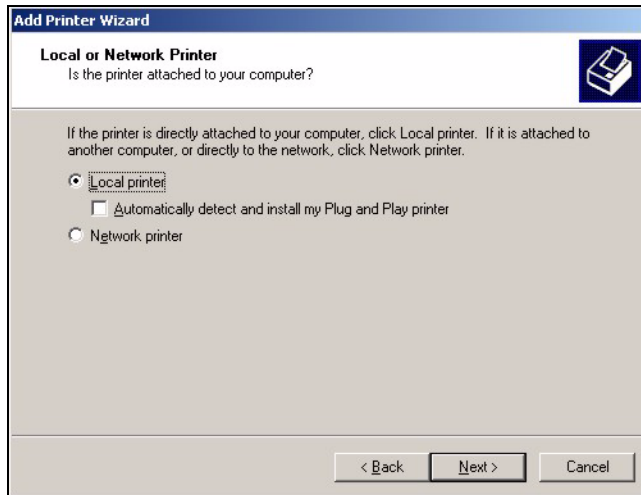
- 2 The **Add Printer Wizard** screen then also displays. Click **Next**.

Figure 70 Add Printer Wizard: Welcome



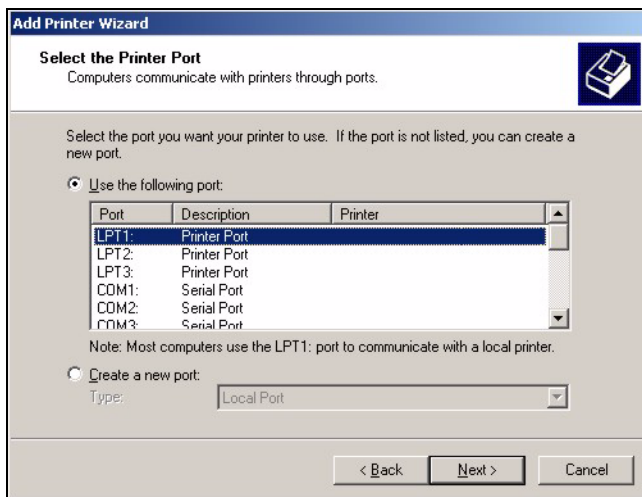
3 Select **Local printer** and click **Next**.

Figure 71 Add Printer Wizard: Local or Network Printer



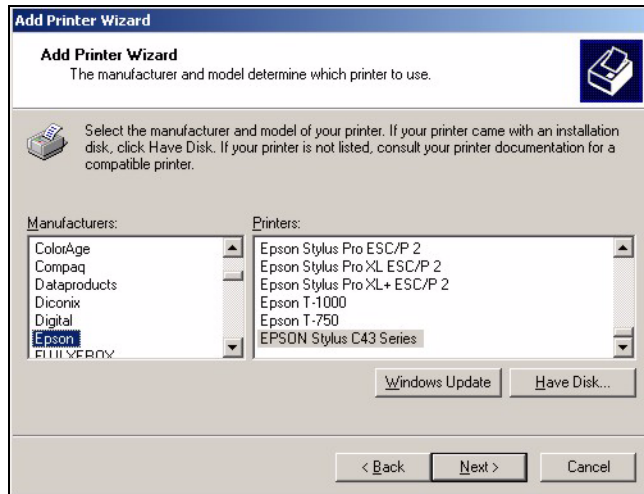
4 Select an **LPT** (Line Printing Terminal) port (a parallel port) as the computer interface for the USB printer.

Figure 72 Add Printer Wizard: Select the Printer Port



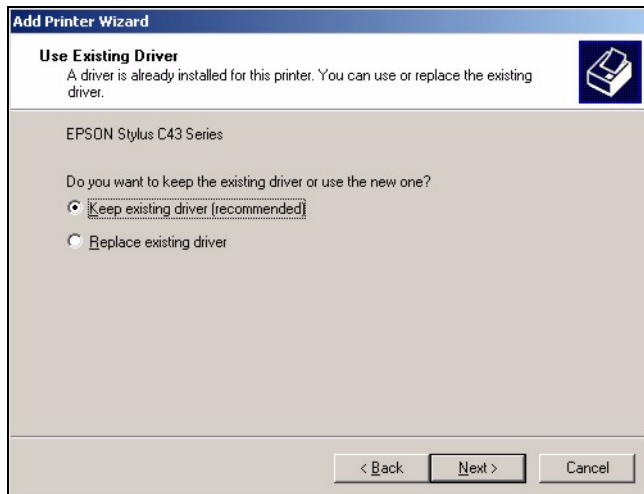
- 5 Select the make of the printer that you want to connect to the print server in the **Manufacturers** list of printers.
- 6 Select the printer model from the list of **Printers**.
- 7 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk...** and install the new printer driver.
- 8 Click **Next** to continue.

Figure 73 Add Printer Wizard: Printer Driver



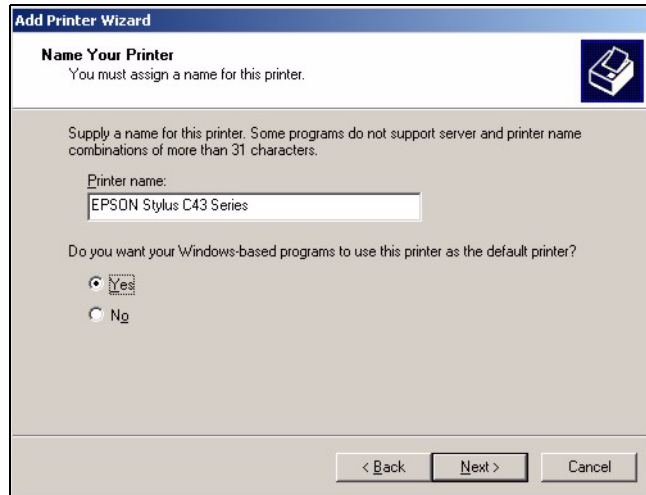
- 9 If the following screen displays, select **Keep existing driver** radio button and click **Next** if you already have a printer driver installed on your computer and you do not want to change it. Otherwise, select **Replace existing driver** to replace it with the new driver you selected in the previous screen and click **Next**.

Figure 74 Add Printer Wizard: Use Existing Driver



10 Type a name to identify the printer and then click **Next** to continue.

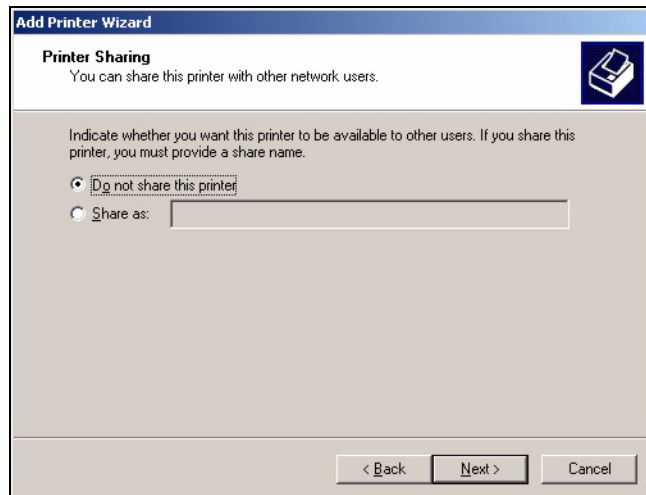
Figure 75 Add Printer Wizard: Name Your Printer



The screenshot shows the 'Add Printer Wizard' dialog box with the 'Name Your Printer' step selected. The title bar reads 'Add Printer Wizard'. Below the title bar, the text says 'Name Your Printer' and 'You must assign a name for this printer.' There is a printer icon in the top right corner. The main area contains the instruction: 'Supply a name for this printer. Some programs do not support server and printer name combinations of more than 31 characters.' Below this is a text box labeled 'Printer name:' containing the text 'EPSON Stylus C43 Series'. Underneath is the question 'Do you want your Windows-based programs to use this printer as the default printer?' with two radio buttons: 'Yes' (which is selected) and 'No'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

11 The ZyXEL Device is a print server itself and you do not need to have your computer act as a print server by sharing the printer with other users in the same network; just select **Do not share this printer** and click **Next** to proceed to the following screen.

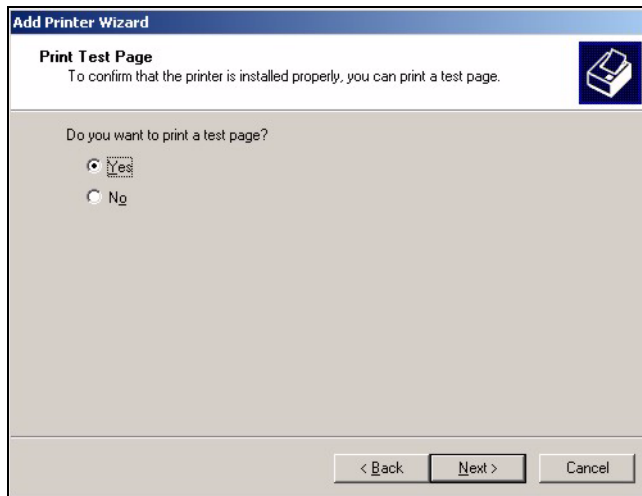
Figure 76 Add Printer Wizard: Printer Sharing



The screenshot shows the 'Add Printer Wizard' dialog box with the 'Printer Sharing' step selected. The title bar reads 'Add Printer Wizard'. Below the title bar, the text says 'Printer Sharing' and 'You can share this printer with other network users.' There is a printer icon in the top right corner. The main area contains the instruction: 'Indicate whether you want this printer to be available to other users. If you share this printer, you must provide a share name.' Below this are two radio buttons: 'Do not share this printer' (which is selected) and 'Share as:'. The 'Share as:' option has an empty text box next to it. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

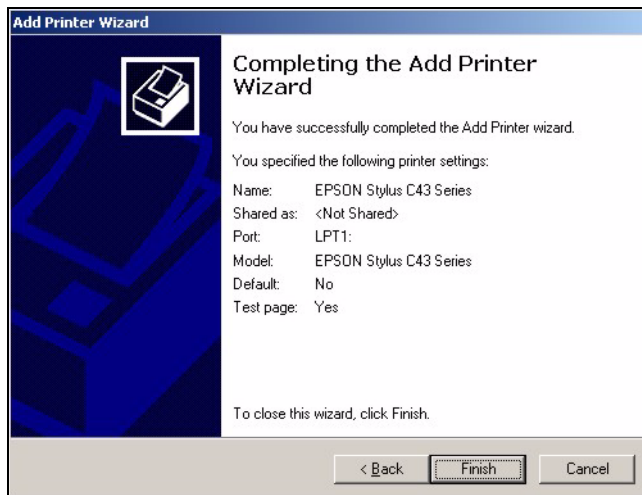
- 12** Select **Yes** and then click the **Next** button if you want to print a test page. A pop-up screen displays to ask if the test page printed correctly. Otherwise select **No** and then click **Next** to continue.

Figure 77 Add Printer Wizard: Print Test Page




- 13** The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.

Figure 78 Add Printer Wizard Complete



16.3 Macintosh OS X

Use the following steps to set up a print server driver on your Macintosh computer.

- 1 Click the **Print Center** icon  located in the Macintosh Dock (a place holding a series of icons/shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.

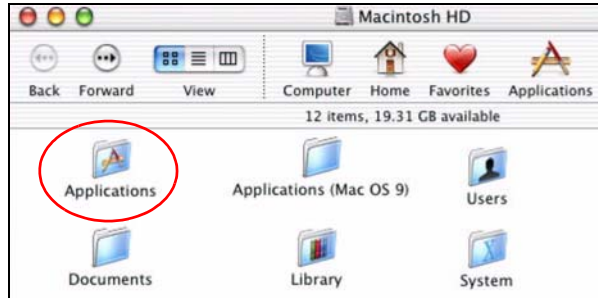
- 2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.

Figure 79 Macintosh HD



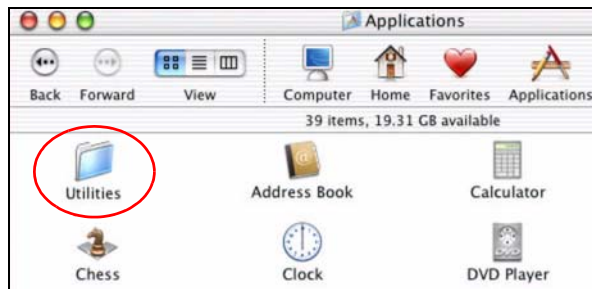
- 3 Double-click the **Applications** folder.

Figure 80 Macintosh HD folder



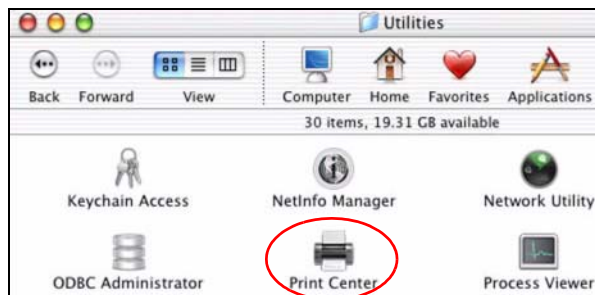
- 4 Double-click the **Utilities** folder.

Figure 81 Applications Folder



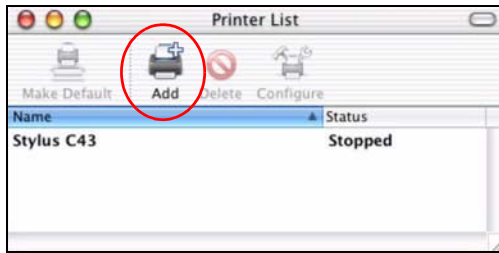
- 5 Double-click the **Print Center** icon.

Figure 82 Utilities Folder



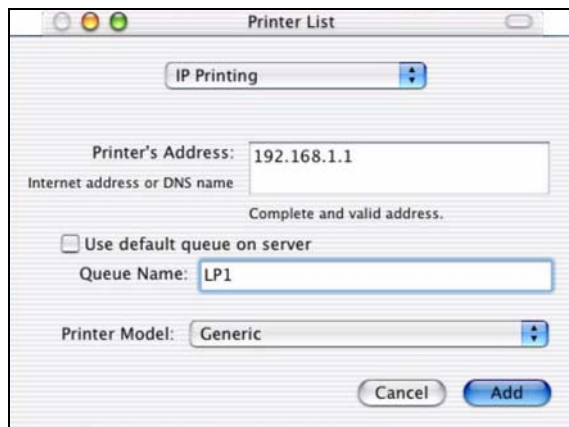
- 6 Click the **Add** icon at the top of the screen.

Figure 83 Printer List Folder



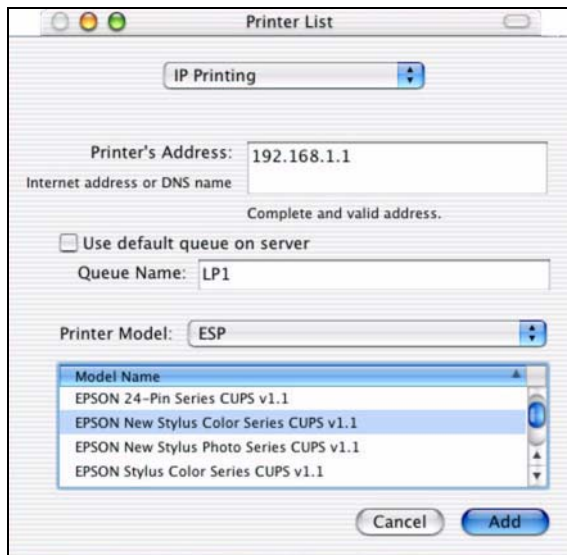
- 7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.
- 8 In the **Printer's Address** field, type the IP address of your ZyXEL Device.
- 9 Deselect the **Use default queue on server** check box.
- 10 Type **LP1** (a parallel port) in the **Queue Name** field.
- 11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.

Figure 84 Printer Configuration



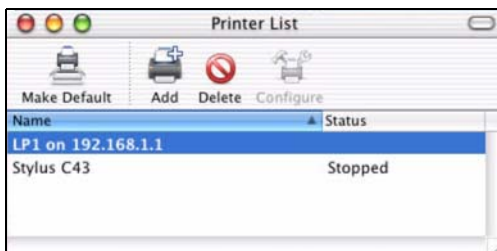
- 12** Click **Add** to select a printer model, save and close the **Printer List** configuration screen.

Figure 85 Printer Model



- 13** The **Name LP1 on 192.168.1.1** displays in the **Printer List** field. The default printer Name displays in bold type.

Figure 86 Print Server



- 14** Your Macintosh print server driver setup is complete. You can now use the ZyXEL Device's print server to print from a Macintosh computer. Refer to the [Chapter 15 on page 131](#) for information on your ZyXEL Device print server configuration screen.

CHAPTER 17

System

This chapter provides information on the System screens.

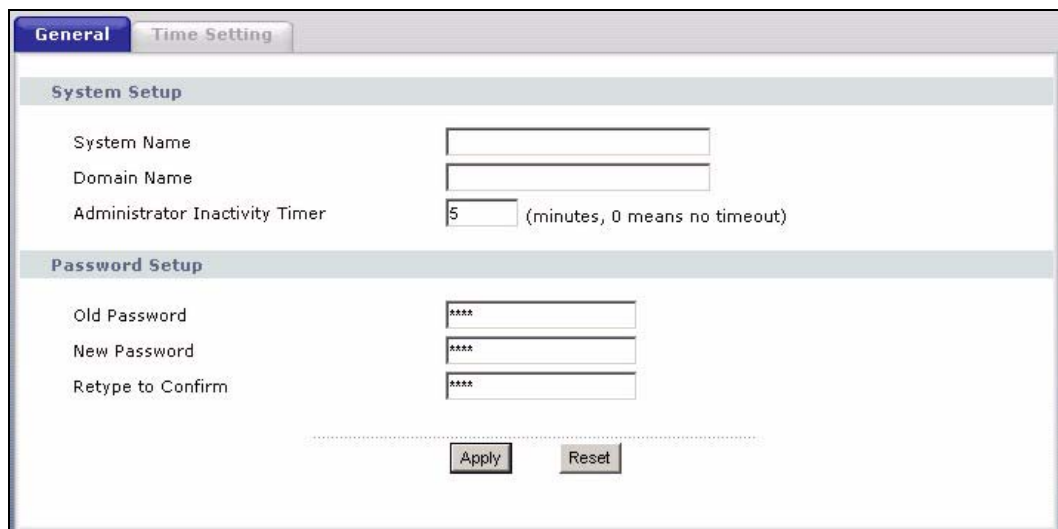
17.1 System Overview

See the chapter about wizard setup for more information on the next few screens.

17.2 System General Screen

Click **Maintenance > System**. The following screen displays.

Figure 87 System General



The screenshot shows a web-based configuration interface for the System General screen. It features two tabs: "General" (selected) and "Time Setting". The main content is divided into two sections: "System Setup" and "Password Setup".

System Setup

System Name	<input type="text"/>
Domain Name	<input type="text"/>
Administrator Inactivity Timer	<input type="text" value="5"/> (minutes, 0 means no timeout)

Password Setup

Old Password	<input type="password" value="****"/>
New Password	<input type="password" value="****"/>
Retype to Confirm	<input type="password" value="****"/>

At the bottom, there are two buttons: "Apply" and "Reset".

The following table describes the labels in this screen.

Table 55 System General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the ZyXEL Device in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	Change your ZyXEL Device's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

17.3 Time Setting Screen

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

Figure 88 Time Setting

The following table describes the labels in this screen.

Table 56 Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
Current Date	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set Time and Date Setup to Manual , enter the new time in this field and then click Apply .

Table 56 Time Setting

LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set Time and Date Setup to Manual , enter the new date in this field and then click Apply .
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.
Auto	Select Auto to have the ZyXEL Device automatically search for an available time server and synchronize the date and time with the time server after you click Apply .
User Defined Time Server Address	Select User Defined Time Server Address and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	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. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Daylight Savings . The o'clock field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, April and type 2 in the o'clock field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Savings . The o'clock field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Last, Sunday, October and type 2 in the o'clock field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 18

Logs

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs. Refer to the appendices for example log message explanations.

18.1 View Log

The web configurator allows you to look at all of the ZyXEL Device's logs in one location.

Click **Maintenance > Logs** to open the **View Log** screen.

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 18.2 on page 152](#)). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 89 View Log

#	Time	Message	Source	Destination	Note
1	04/06/2006 14:28:47	Successful WEB login	192.168.1.33		User:admin
2	04/06/2006 14:18:15	Time synchronization successful			
3	04/06/2006 14:18:15	Time initialized by NTP server: ntp3.cs.wisc.edu	128.105.37.11:123	172.23.23.114:123	
4	04/06/2006 14:17:13	Time synchronization successful			
5	04/06/2006 14:17:13	Time initialized by NTP server: ntp3.cs.wisc.edu	128.105.37.11:123	172.23.23.114:123	
6	04/06/2006 06:11:52	Time synchronization successful			
7	04/06/2006 06:11:52	Time initialized by NTP server: time1.stupi.se	192.36.143.150:123	172.23.23.114:123	
8	01/01/2000 04:50:52	WAN interface gets IP:172.23.23.114			WAN1
9	01/01/2000 04:23:06	Successful WEB login	192.168.1.33		User:admin
10	01/01/2000 03:43:10	Waiting content filter server (66.35.255.70) timeout!	192.168.1.33:3241	202.43.201.234:80	tw.f172.mail.yahoo.com
11	01/01/2000 03:42:02	Waiting content filter server (66.35.255.70) timeout!	192.168.1.33:3188	203.84.196.97:80	tw.yimg.com

The following table describes the labels in this screen.

Table 57 View Logs

LABEL	DESCRIPTION
Display	The categories that you select in the Log Settings page (see Section 18.2 on page 152) display in the drop-down list box. Select a category of logs to view; select All Logs to view logs from all of the log categories that you selected in the Log Settings page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the ZyXEL Device's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click Email Log Now to send the log screen to the e-mail address specified in the Log Settings page (make sure that you have first filled in the Address Info fields in Log Settings).
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.

18.2 Log Settings

You can configure the ZyXEL Device's general log settings in one location.

Click **Maintenance > Logs > Log Settings** to open the **Log Settings** screen.

Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 90 Log Settings

The screenshot shows the 'Log Settings' configuration page. It has a 'View Log' button and a 'Log Settings' tab. The page is organized into three main sections:

- E-mail Log Settings:** Contains input fields for 'Mail Server' (with a note: '(Outgoing SMTP Server NAME or IP Address)'), 'Mail Subject', 'Send Log to' (with a note: '(E-Mail Address)'), and 'Send Alerts to' (with a note: '(E-Mail Address)'). It also includes a checkbox for 'SMTP Authentication' with sub-fields for 'User Name' and 'Password'. There are dropdown menus for 'Log Schedule' (set to 'None') and 'Day for Sending Log' (set to 'Sunday'). Two input boxes for 'Time for Sending Log' are set to '0' for both 'hour' and 'minute'. A checkbox 'Clear log after sending mail' is present.
- Syslog Logging:** Includes a checkbox for 'Active', an input field for 'Syslog Server IP Address' (set to '0.0.0.0' with a note: '(Server NAME or IP Address)'), and a dropdown for 'Log Facility' (set to 'Local 1').
- Active Log and Alert:** Features two columns of checkboxes. The left column includes: System Maintenance (checked), System Errors (checked), Access Control, TCP Reset, Packet Filter, ICMP, Remote Management, CDR (checked), PPP (checked), UPnP, Forward Web Sites, Blocked Web Sites, Blocked Java etc., and Attacks. The right column includes: Send immediate alert, System Errors, Access Control, Blocked Web Sites, Blocked Java etc., and Attacks.

At the bottom of the page are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 58 Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends.
Send Log To	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.

Table 58 Log Settings

LABEL	DESCRIPTION
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. If you select Weekly or Daily , specify a time of day when the E-mail should be sent. If you select Weekly , then also specify which day of the week the E-mail should be sent. If you select When Log is Full , an alert is sent when the log fills up. If you select None , no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click Active to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 19

Tools

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the ZyXEL Device.

19.1 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "ZyXEL Device.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **Maintenance > Tools**. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 91 Maintenance Firmware Upload

The following table describes the labels in this screen.

Table 59 Maintenance Firmware Upload

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

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

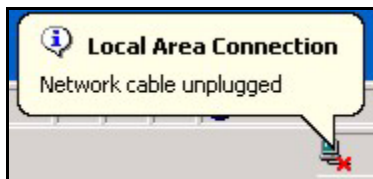
After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 92 Upload Warning



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 93 Network Temporarily Disconnected



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

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

Figure 94 Upload Error Message



19.2 Configuration Screen

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

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 95 Configuration

The screenshot shows the Configuration page with the following sections:

- Backup Configuration:** "Click **Backup** to save the current configuration of your system to your computer." with a **Backup** button.
- Restore Configuration:** "To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload." with a "File Path:" input field, a **Browse...** button, and an **Upload** button.
- Back to Factory Defaults:** "Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the
 - Password will be 1234
 - LAN IP address will be 192.168.1.1
 - DHCP will be reset to server
 with a **Reset** button.

19.2.1 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

19.2.2 Restore Configuration

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

Table 60 Maintenance Restore Configuration

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

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

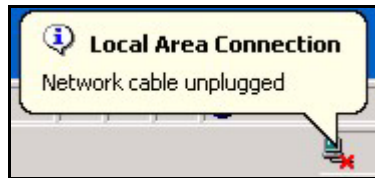
After you see a “configuration upload successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 96 Configuration Restore 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 97 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 your Quick Start Guide for details on how to set up your computer's IP address.

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

Figure 98 Configuration Restore Error



19.2.3 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.

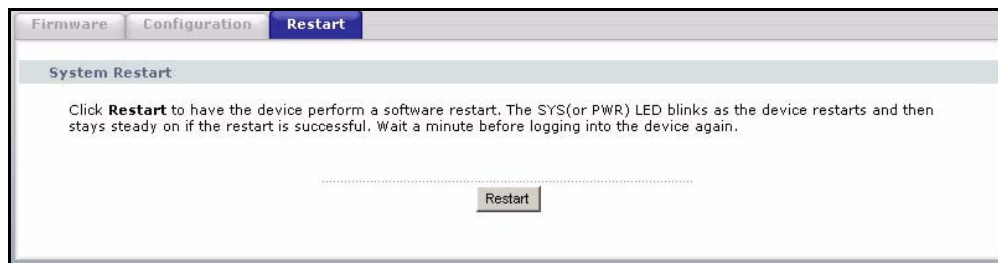
You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

19.3 Restart Screen

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

Click **Maintenance > Tools > Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 99 System Restart

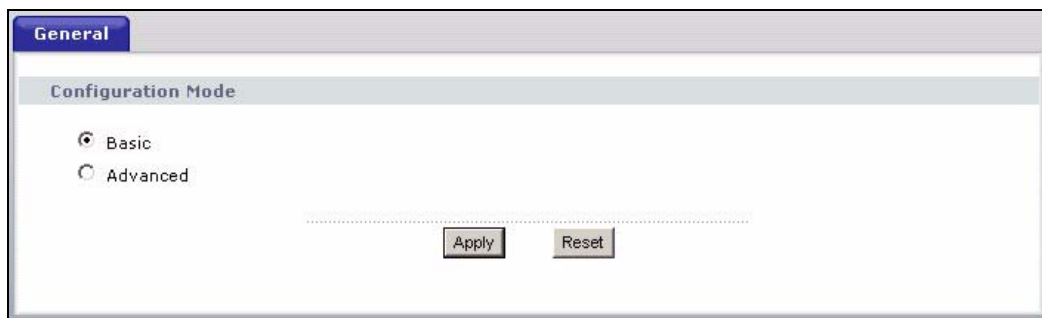


CHAPTER 20

Configuration Mode

Click **Maintenance > Config Mode** to open the following screen. This screen allows you to hide or display the advanced screens of some features or the advanced features, such as MAC filter or static route. **Basic** is selected by default and you cannot see the advanced screens or features. If you want to view and configure all screens including the advanced ones, select **Advanced** and click **Apply**.

Figure 100 Config Mode



The following table includes the screens that you can view and configure only when you select **Advanced**.

Table 61 Config Mode: Advanced Screens

CATEGORY	LINK	TAB
Network	WAN	Advanced
	LAN	IP Alias
		Advanced
	DHCP Server	Advanced
	NAT	Advanced
Security	Firewall	Services
	Content Filter	Schedule
Management	Static Route	IP Static Route
	Bandwidth MGMT	Advanced
		Monitor
	Remote MGMT	Telnet
		FTP
DNS		
Maintenance	Logs	Log Settings

CHAPTER 21

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

21.1 Problems Starting Up the ZyXEL Device

Table 62 Troubleshooting Starting Up 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. Make sure 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>

21.2 Problems with the LAN

Table 63 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	<p>Check your Ethernet cable connections (refer to the Quick Start Guide for details). Check for faulty Ethernet cables.</p>
	<p>Make sure your computer's Ethernet Card is working properly.</p>
I cannot access the ZyXEL Device from the LAN.	<p>If Any IP is disabled, make sure that the IP address and the subnet mask of the ZyXEL Device and your computer(s) are on the same subnet.</p>

21.3 Problems with the WAN

Table 64 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The WAN LED is off.	Check the connections between the ZyXEL Device WAN port and the cable/DSL modem or ethernet jack.
	Check whether your cable/DSL device requires a crossover or straight-through cable.
I cannot get a WAN IP address from the ISP.	Click WAN to verify your settings. The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct Service Type, User Name and Password (be sure to use the correct casing). Refer to the WAN Setup chapter.
I cannot access the Internet.	Make sure the ZyXEL Device is turned on and connected to the network. Verify your WAN settings. Refer to the chapter on WAN setup. Make sure you entered the correct user name and password. If you use PPPoE pass through, make sure that bridge mode is turned on.
The Internet connection disconnects.	If you use PPPoE encapsulation, check the idle time-out setting. Refer to the Chapter 4 on page 57 . Contact your ISP.

21.4 Problems with Restricted Web Pages and Keyword Blocking

Table 65 Troubleshooting Restricted Web Pages and Keyword Blocking

PROBLEM	CORRECTIVE ACTION
Access to a restricted web page is not blocked.	Make sure that the Enable Parental Control check box is selected in the Parental Control screen.
	Make sure that you select a category in the Parental Control screen to restrict access to web pages relevant to that category. For example, select the Gambling check box to prevent access to www.onlinegambling.com .
Access to a web page with a URL containing a forbidden keyword is not blocked.	Make sure that you select the Keyword Blocking check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the Keyword List.
	If a keyword that is listed in the Keyword List is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filter chapter.

Table 65 Troubleshooting Restricted Web Pages and Keyword Blocking

PROBLEM	CORRECTIVE ACTION
Parental Control is configured correctly, but I can still access restricted web pages.	Restart the device to clear the cache.
	The content filter server may be unavailable. The View Logs screen can display content filtering log messages. See the Log Descriptions appendix for a list of possible log messages. In the View Logs screen copy and paste the log messages and e-mail them to customer support with an explanation of the problem.
	If you still have problems, contact your vendor or customer support for further advice.

21.5 Problems with the Password

Table 66 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyXEL Device.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	Use the Reset button to restore the factory default configuration file. This will restore all of the factory defaults including the password; see section 2.3 for details.

21.6 Problems with the Print Server

Table 67 Troubleshooting the Print Server

PROBLEM	CORRECTIVE ACTION
Cannot print anything using the USB printer connected to the P-335U.	Verify that the printer uses USB 1.1 or 1.0 by checking your printer's specifications.
	Make sure the USB printer is powered on and can work properly.
	Make sure you install the print server driver on your computer. See Chapter 16 on page 133 for how to set up the print server driver on your computer.
	Check the USB cable connections.

21.7 Problems with Remote Management

Table 68 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyXEL Device from the LAN or WAN.	Refer to Chapter 13 on page 117 for scenarios when remote management may not be possible.
	When NAT is enabled: <ul style="list-style-type: none"> • 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.

21.8 Problems Accessing the ZyXEL Device

Table 69 Troubleshooting Accessing the ZyXEL Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	The username is "admin". The default password is "1234". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.
I cannot access the web configurator.	Make sure that there is not a Telnet console session running. Use the ZyXEL Device's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection. Use the ZyXEL Device's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection. 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. 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 the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.

21.8.1 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.

21.8.1.1 Internet Explorer Pop-up Blockers

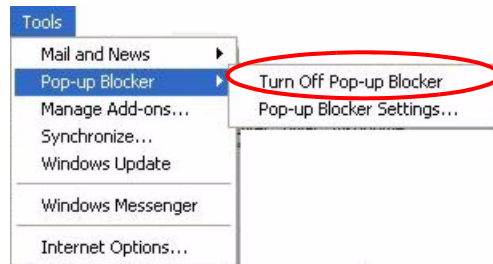
You may have to disable pop-up blocking to log into your device.

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.

21.8.1.1.1 Disable pop-up Blockers

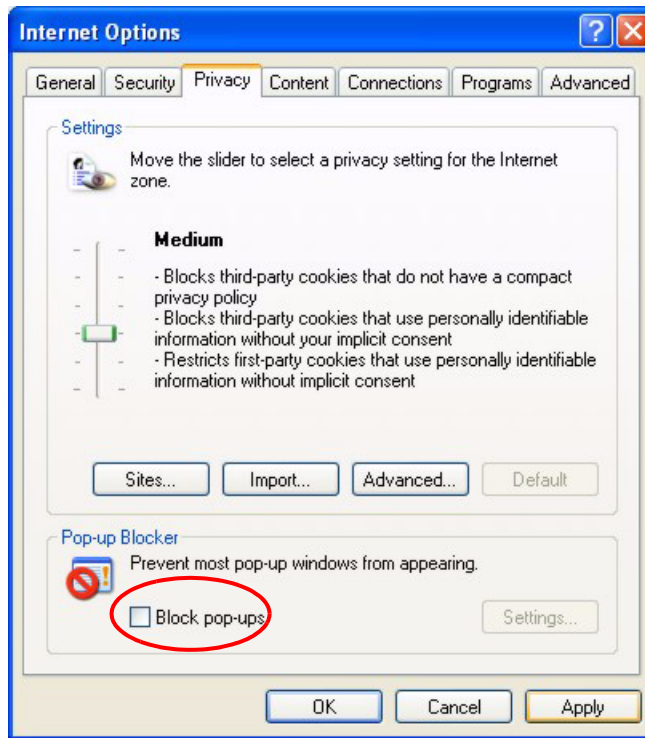
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 101 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.

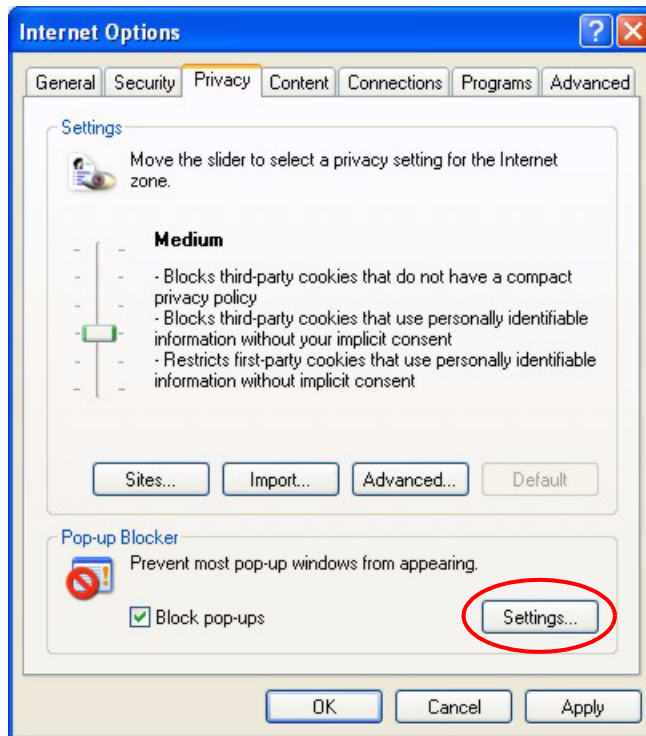
Figure 102 Internet Options

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

21.8.1.1.2 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 103 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**.

Note: If you change the IP address of your device, make sure that the new address matches the address you type in the **Pop-up Blocker Settings** screen.

Figure 104 Pop-up Blocker Settings

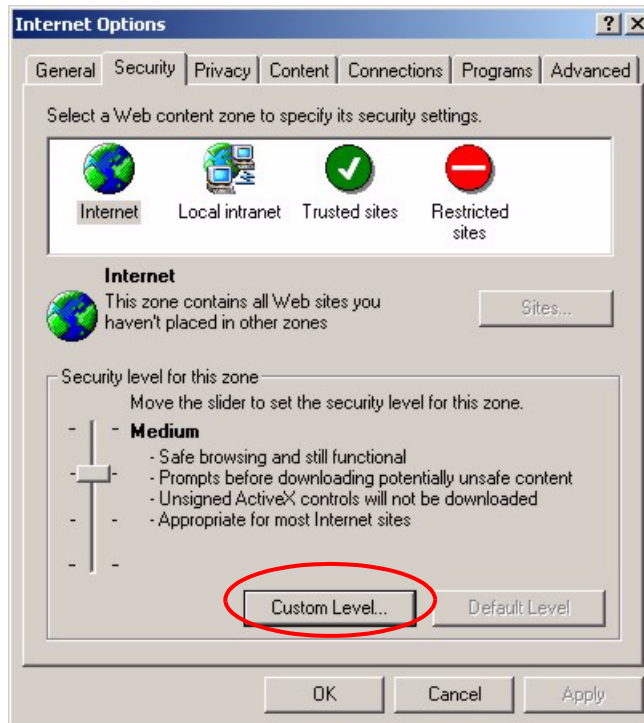
5 Click **Close** to return to the **Privacy** screen.

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

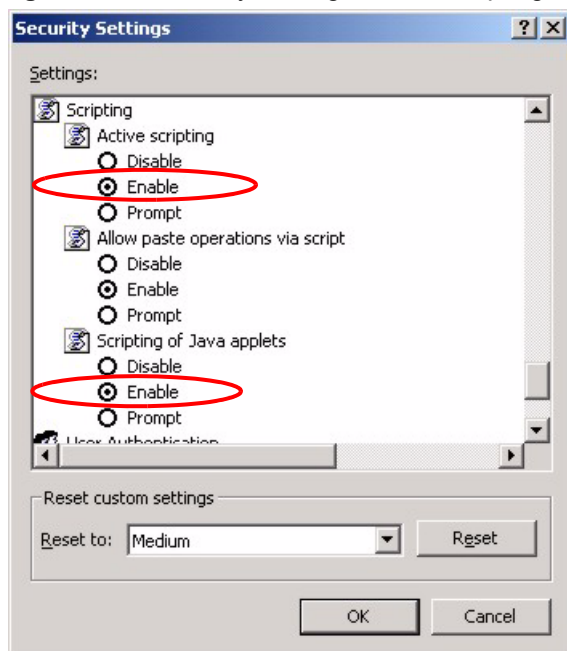
21.8.1.2 JavaScripts

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.

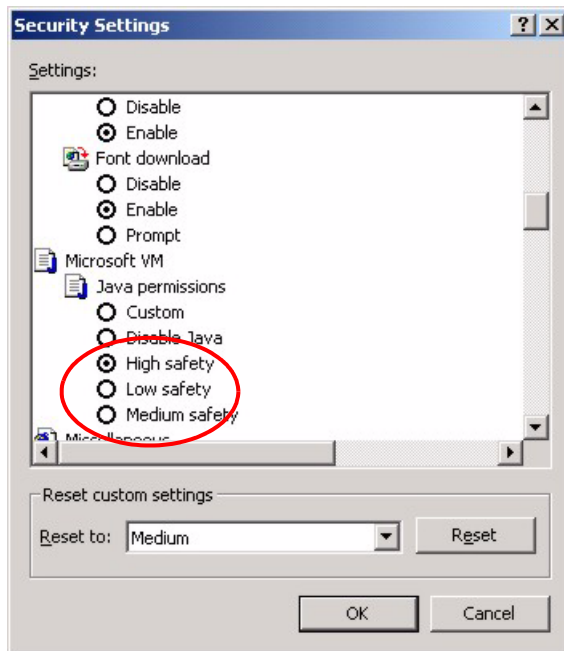
Figure 105 Internet Options

- 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 106 Security Settings - Java Scripting

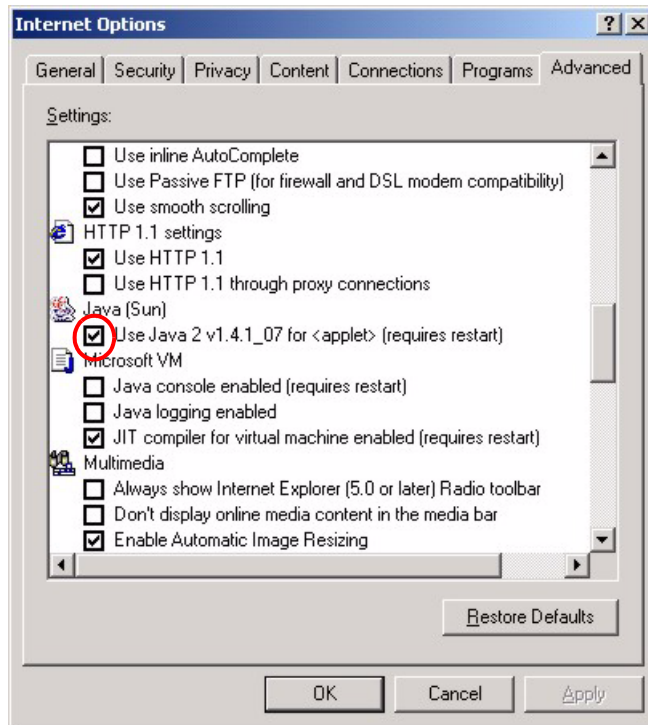
21.8.1.3 Java Permissions

- 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 107 Security Settings - Java

21.8.1.3.1 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.

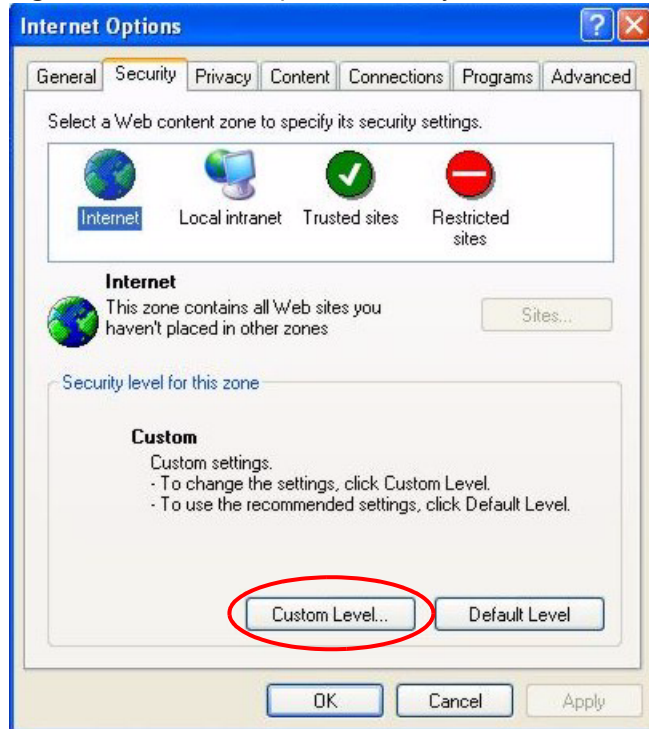
Figure 108 Java (Sun)

21.8.2 ActiveX Controls in Internet Explorer

If ActiveX is disabled, you will not be able to download ActiveX controls or to use Trend Micro Security Services. Make sure that ActiveX controls are allowed in Internet Explorer.

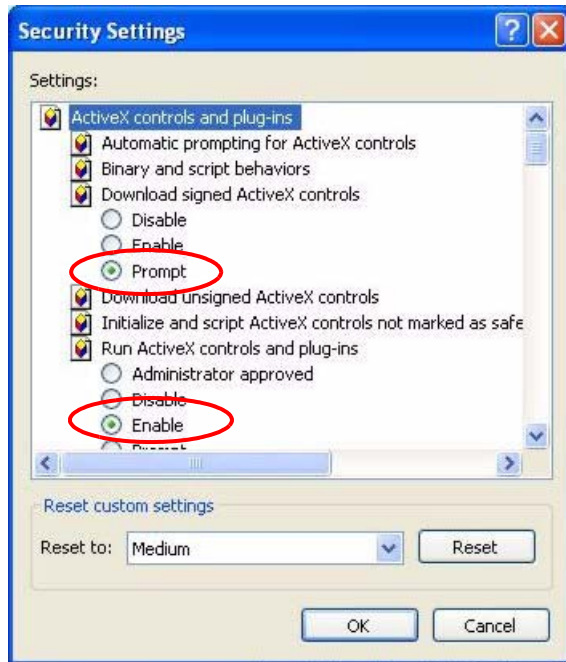
Screen shots for Internet Explorer 6 are shown. Steps may vary depending on your version of Internet Explorer.

- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 In the **Internet Options** window, click **Custom Level**.

Figure 109 Internet Options Security

- 3** Scroll down to **ActiveX controls and plug-ins**.
- 4** Under **Download signed ActiveX controls** select the **Prompt** radio button.
- 5** Under **Run ActiveX controls and plug-ins** make sure the **Enable** radio button is selected.
- 6** Then click the **OK** button.

Figure 110 Security Setting ActiveX Controls



APPENDIX A

Product Specifications

The following table is a summary of other features available.

Table 70 Hardware Features

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
Dimensions (W x D x H)	190 x 128 x 33 mm
Power Specification	12 V AC 1 A
Ethernet ports	Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
USB Port	USB version 1.1.
Operation Temperature	0° C ~ 50° C
Storage Temperature	-20° C ~ 60° C
Operation Humidity	20% ~ 95% RH
Storage Humidity	10% ~ 90% RH
Distance between the centers of the holes on the device's back.	125 mm
Screw size for wall-mounting	M 3*10

Table 71 Firmware Features

FEATURE	DESCRIPTION
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration and put it back on the ZyXEL Device later if you decide you want to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.

Table 71 Firmware Features

FEATURE	DESCRIPTION
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP Alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the ZyXEL Device itself as the gateway for each subnet.
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the ZyXEL Device to an external UNIX syslog server.
PPPoE	PPPoE mimics a dial-up over Ethernet Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The ZyXEL Device supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The ZyXEL Device can communicate with other UPnP enabled devices in a network.
RoadRunner Support	In addition to standard cable modem services, the ZyXEL Device supports Time Warner's RoadRunner Service.

APPENDIX B

Print Server Specifications

This appendix provides details on the print server interface and system requirements.

Table 72 Print Server Interface

PRINT SERVER INTERFACE	
USB	USB 1.1 (full speed) - compliant port, 1.5Mbps (low speed) and 12Mbps (full speed) data transmission rates. This port automatically detects the make and model of the USB printer connected to this port.

Table 73 Print Server Requirements and Specifications

PRINT SERVER REQUIREMENTS AND SPECIFICATIONS	
Network Operating System Support	Windows 95/98/98SE/Me Windows NT 4.0/2000/XP/2003 Mac OS X or higher
Network Protocol Support ^a	Print Monitor: UDP <ul style="list-style-type: none"> • Windows 95/98/98SE/Me • Windows NT 4.0/2000/XP/2003 LPD/LPR (RFC 1179): TCP/IP <ul style="list-style-type: none"> • Windows NT 4.0/2000/XP/2003 • Mac OS X or higher
DHCP (client) Support	Yes
Management	Web interface Windows-based wizard program

a. Only a printer with a USB connection can be used with the ZyXEL Device.

ZyXEL Device Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the ZyXEL Device print server.

Table 74 Compatible USB Printers

BRAND	MODEL	TYPE	REMARK
CANON	BJ F9000	Inkjet	
CANON	i2355	Inkjet	
CANON	i255	Inkjet	
CANON	i320	Inkjet	
CANON	i355	Inkjet	
CANON	i450	Inkjet	
CANON	i455	Inkjet	
CANON	i470D	Inkjet	
CANON	i475D	Inkjet	
CANON	i550	Inkjet	
CANON	i560	Inkjet	
CANON	i6100	Inkjet	
CANON	i6500	Inkjet	
CANON	i850	Inkjet	
CANON	i865	Inkjet	
CANON	i9100	Inkjet	
CANON	i950	Inkjet	
CANON	i9950	Inkjet	
CANON	S200SPx	Inkjet	
CANON	S200SRx	Inkjet	
CANON	S520	Inkjet	
CANON	PIXMA ip1000	Inkjet	
CANON	PIXMA ip2000	Inkjet	
CANON	PIXMA ip3000	Inkjet	
CANON	PIXMA ip4000	Inkjet	
CANON	PIXMA ip5000	Inkjet	
CANON	PIXMA ip6000D	Inkjet	
CANON	PIXMA ip8500	Inkjet	
CANON	MP-110	MFP	

Table 74 Compatible USB Printers

BRAND	MODEL	TYPE	REMARK
CANON	MP-130	MFP	
EPSON	Aculaser C1900	Color Laser	
EPSON	EPL-6100	Laser	Disable bi-directional support on printer.
EPSON	Stylus C20	Inkjet	Disable bi-directional support on printer.
EPSON	Stylus C20SX	Inkjet	Disable bi-directional support on printer.
EPSON	Stylus C40	Inkjet	Disable bi-directional support on printer.
EPSON	Stylus C43UX	Inkjet	
EPSON	Stylus C60	Inkjet	Disable bi-directional support on printer.
EPSON	Stylus C63	Inkjet	
EPSON	Stylus C83	Inkjet	
EPSON	Stylus Color 1160	Inkjet	Disable bi-directional support on printer.
EPSON	Stylus Color 670	Inkjet	
EPSON	Stylus Color 800	Inkjet	Disable printer status monitor.
EPSON	Stylus Color 810	Inkjet	
EPSON	Stylus Photo 915	Inkjet	
EPSON	Stylus Photo1270	Inkjet	
EPSON	Stylus Photo2100	Inkjet	
EPSON	Stylus Photo810	Inkjet	
EPSON	Stylus PhotoEX3	Inkjet	
EPSON	EPL-5900	Laser	
EPSON	Stylus Photo1270	Inkjet	
EPSON	EPL-6200	Laser	
EPSON	LP 2500	Laser	
EPSON	LP 8900	Laser	
EPSON	Stylus Photo830U	Inkjet	
EPSON	TM-T88III	Thermo	
HP	DeskJet 1125C	Inkjet	Change data type to EMF and disable bi-directional support on printer.
HP	DeskJet 1220C	Inkjet	Change data type to EMF and disable bi-directional support on printer.
HP	DeskJet 3650	Inkjet	

Table 74 Compatible USB Printers

BRAND	MODEL	TYPE	REMARK
HP	DeskJet 5550	Inkjet	
HP	DeskJet 810C	Inkjet	
HP	DeskJet 845C	Inkjet	
HP	DeskJet 920C	Inkjet	
HP	Deskjet 1180c	Inkjet	
HP	DeskJet 930C	Inkjet	
HP	LaserJet 1200	Laser	Disable bi-directional support on printer.
HP	LaserJet 1220	Laser	Disable bi-directional support on printer.
HP	LaserJet 1300	Laser	
HP	LaserJet 2200	Laser	Disable bi-directional support on printer.
HP	LaserJet 2200D	Laser	Disable bi-directional support on printer.
HP	LaserJet 3330	Laser	
HP	LaserJet 5000	Color Laser	Requires PCL5 or PCL6 printer driver.
HP	LaserJet 5000LE	Color Laser	Requires PCL5 or PCL6 printer driver.
HP	Photosmart 7150	Inkjet	
HP	Photosmart 2610	MFP	
HP	LaserJet 1500L	Color Laser	
HP	PSC 1315	MFP	
HP	DeskJet 3535	Inkjet	
HP	DeskJet 5550	Inkjet	
HP	DeskJet 5652	Inkjet	
HP	LaserJet 2300	Laser	
HP	LaserJet 2420	Laser	
HP	LaserJet 4250	Laser	
HP	LaserJet 2550	Color Laser	
HP	LaserJet 3015	MFP	
IBM	Infoprint 1332	Laser	
IBM	Infoprint 1412	Laser	
KYOCERA	FS-1010	Laser	
KYOCERA	FS-1020D	Laser	

Table 74 Compatible USB Printers

BRAND	MODEL	TYPE	REMARK
KYOCERA	FS-1920	Laser	
KONICA MINOLTA	PagePro 1350W	Laser	
LEXMARK	C750	Color Laser	
LEXMARK	E210	Laser	
LEXMARK	E322	Laser	
LEXMARK	T420	Laser	
LEXMARK	T620	Laser	
LEXMARK	W812	Laser	
LEXMARK	Z42	Inkjet	
LEXMARK	Z43	Inkjet	
LEXMARK	Z45	Inkjet	
LEXMARK	Z55	Inkjet	
LEXMARK	Z705	Inkjet	
LEXMARK	E230	Laser	
LEXMARK	X6170	MFP	
LEXMARK	Z515	Inkjet	
OKI	B4350	Laser	
SAMSUNG	ML-1710	Laser	
SAMSUNG	ML-1750	Laser	
SAMSUNG	CLP-510	Laser	
SAMSUNG	SCX-4016	MFP	
SHARP	AR-M160	MFP	
SHARP	AR-M205	MFP	
XEROX	Phaser 3310	Laser	
XEROX	DocuPrint 240A	Laser	
PS: For MFP, the print server supports the printing function only.			

APPENDIX C

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

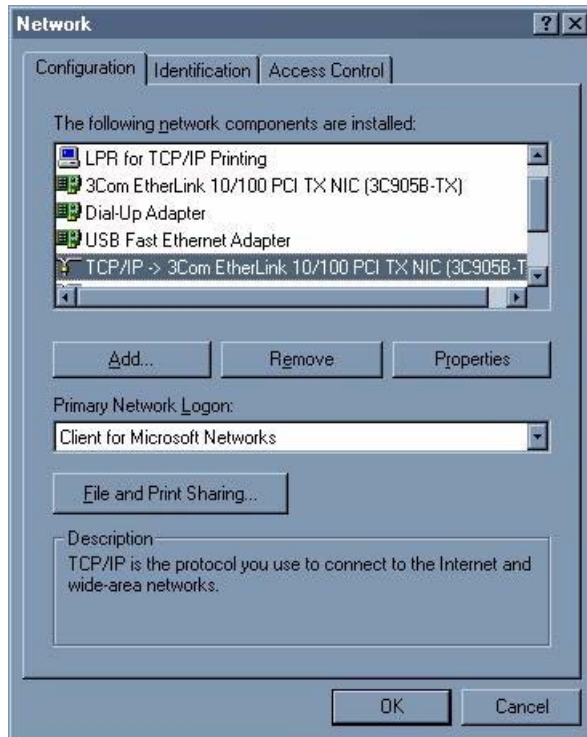
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the 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 111 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:

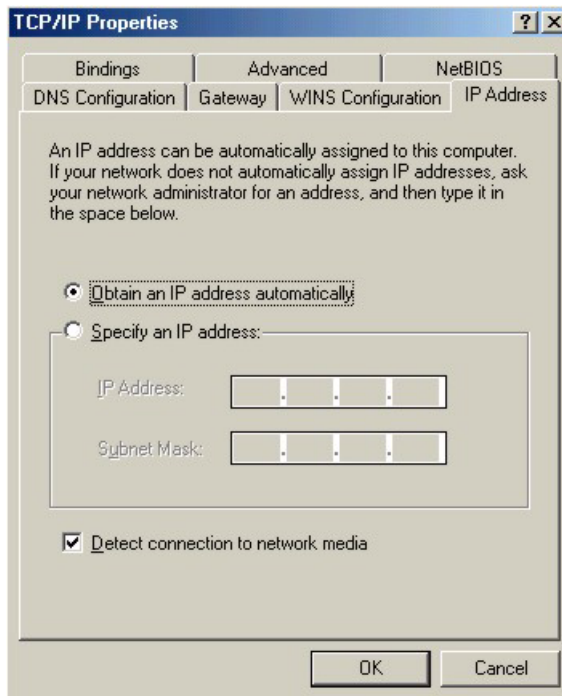
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

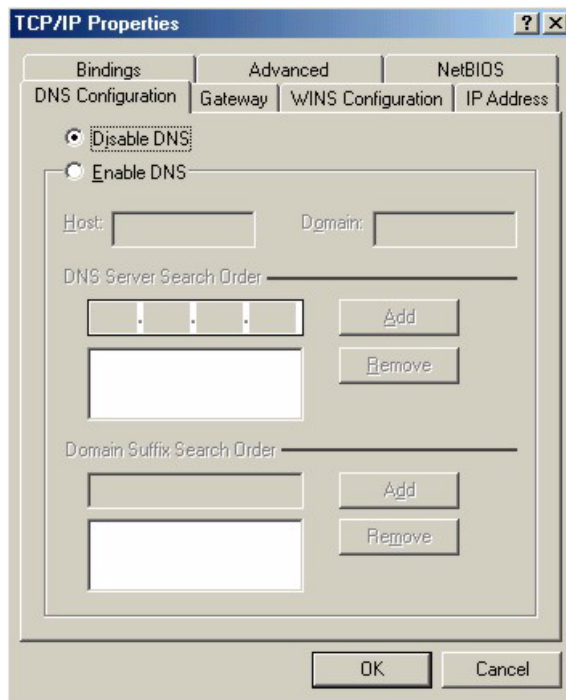
Configuring

- 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 112 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 113 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.

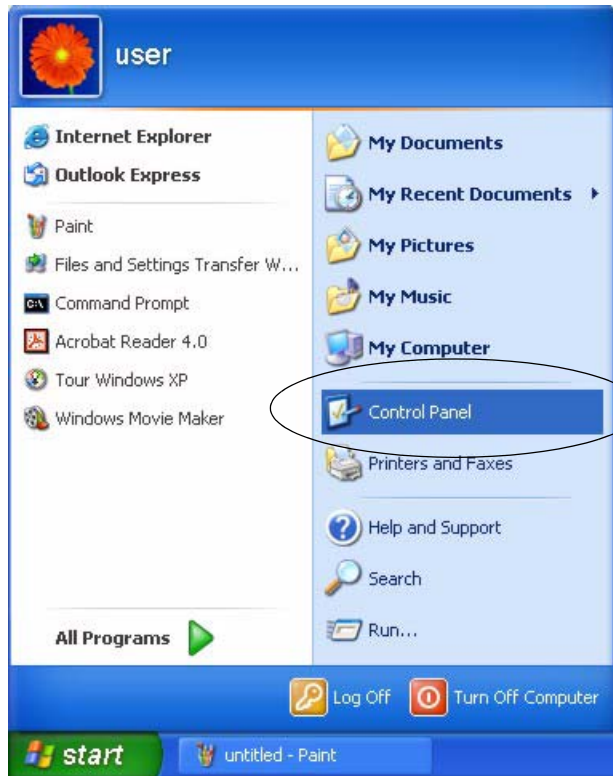
Verifying Settings

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.

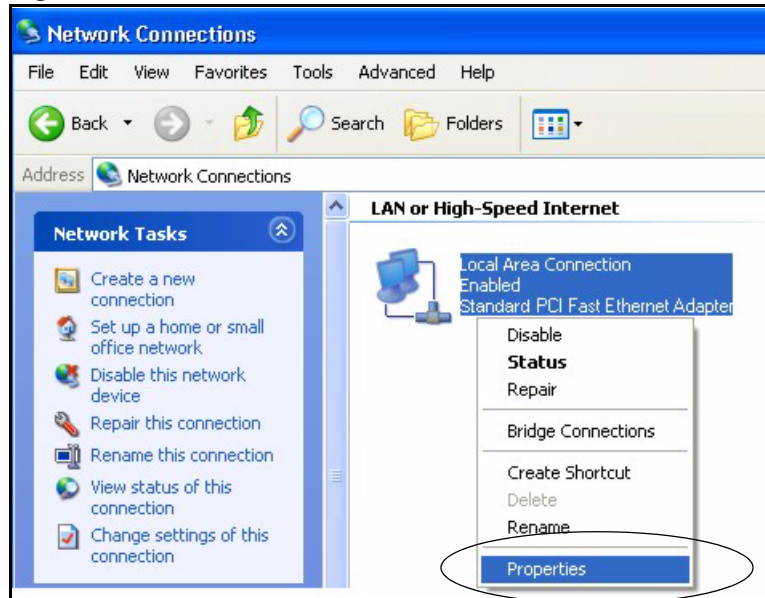
1 Click **start** (**Start** in Windows 2000/NT), **Settings, Control Panel**.

Figure 114 Windows XP: Start Menu

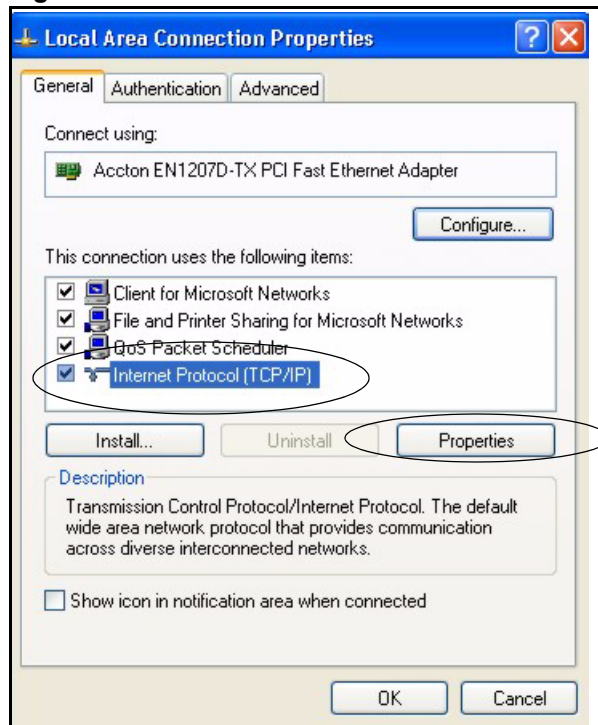
2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

Figure 115 Windows XP: Control Panel

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

Figure 116 Windows XP: Control Panel: Network Connections: Properties

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

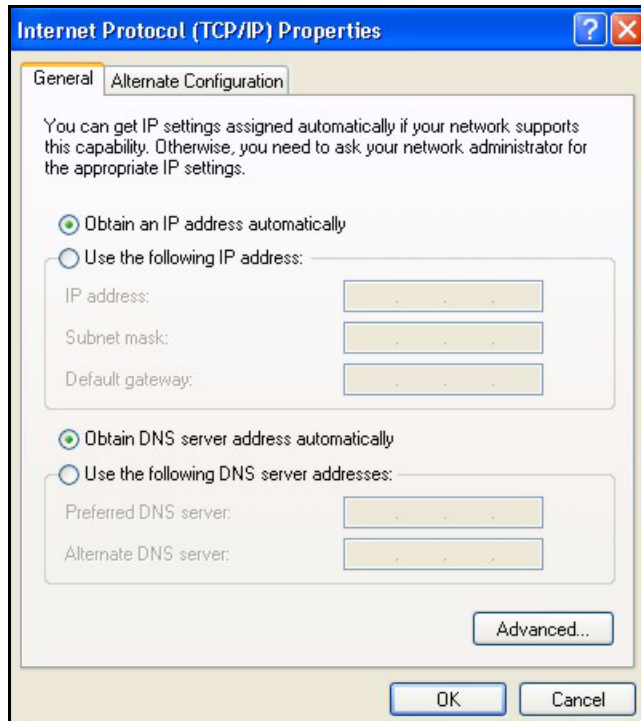
Figure 117 Windows XP: Local Area Connection Properties

- 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**.

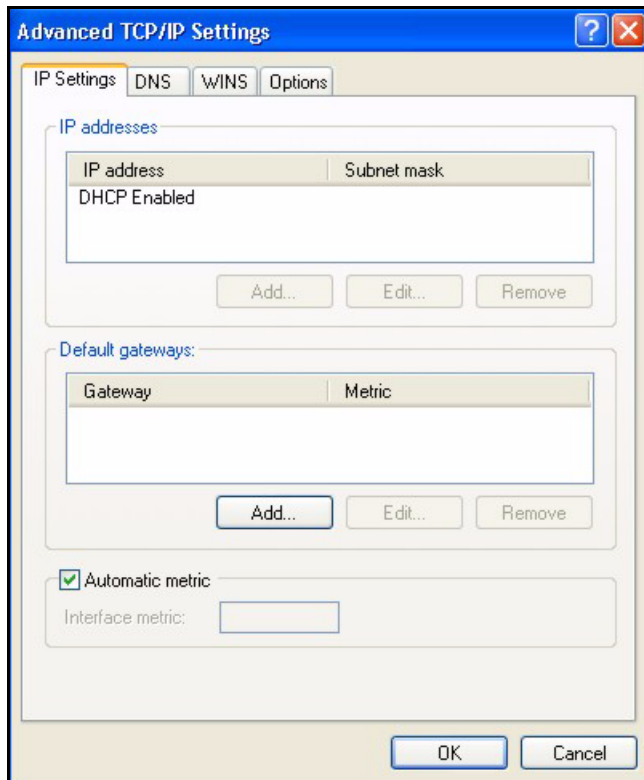
Figure 118 Windows XP: Internet Protocol (TCP/IP) Properties



- 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:

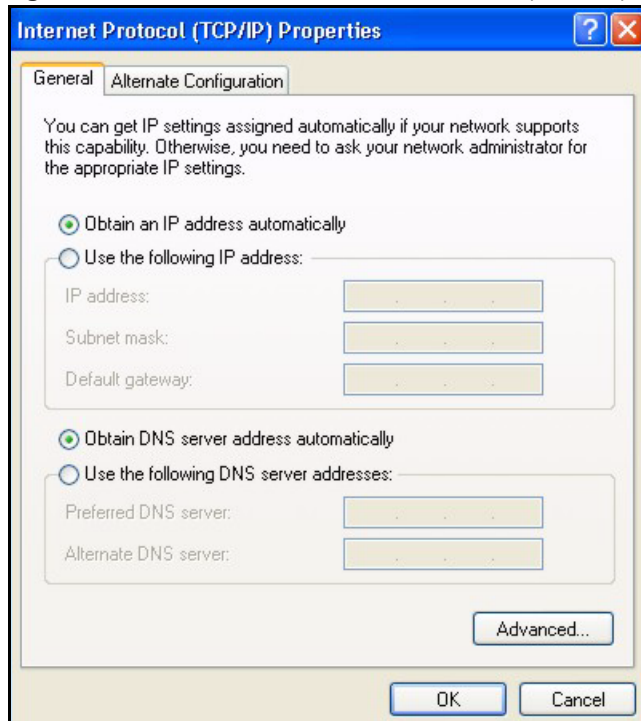
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP 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 119 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 120 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).

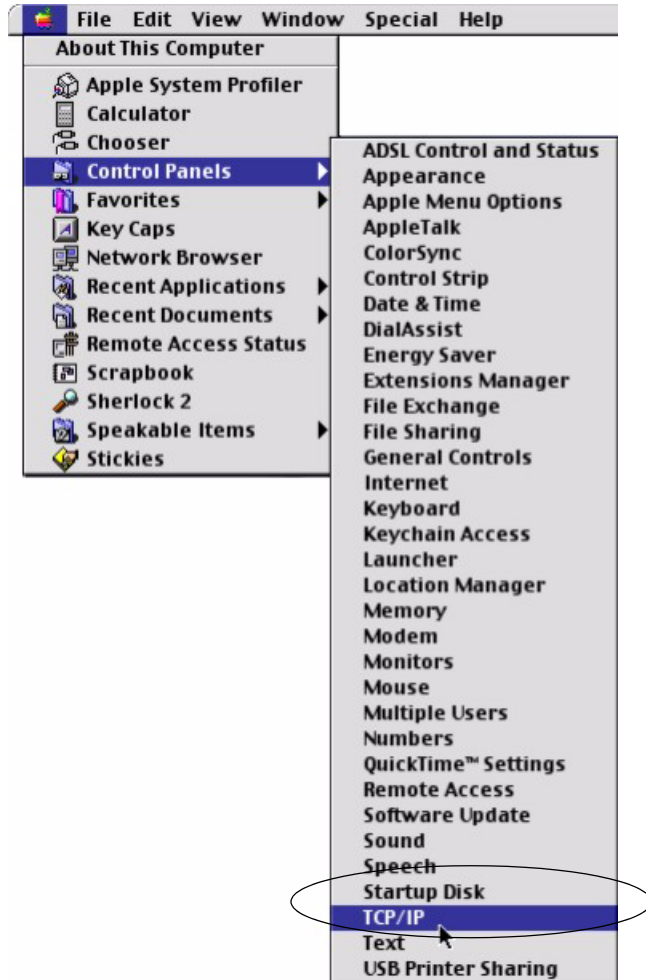
Verifying Settings

- 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

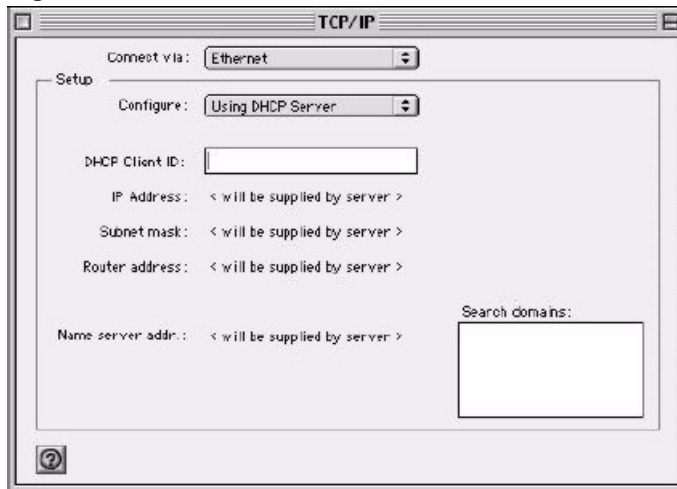
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 121 Macintosh OS 8/9: Apple Menu



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

Figure 122 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).

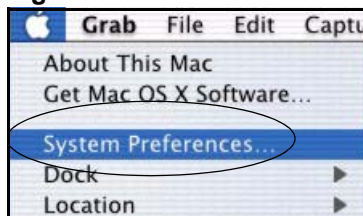
Verifying Settings

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

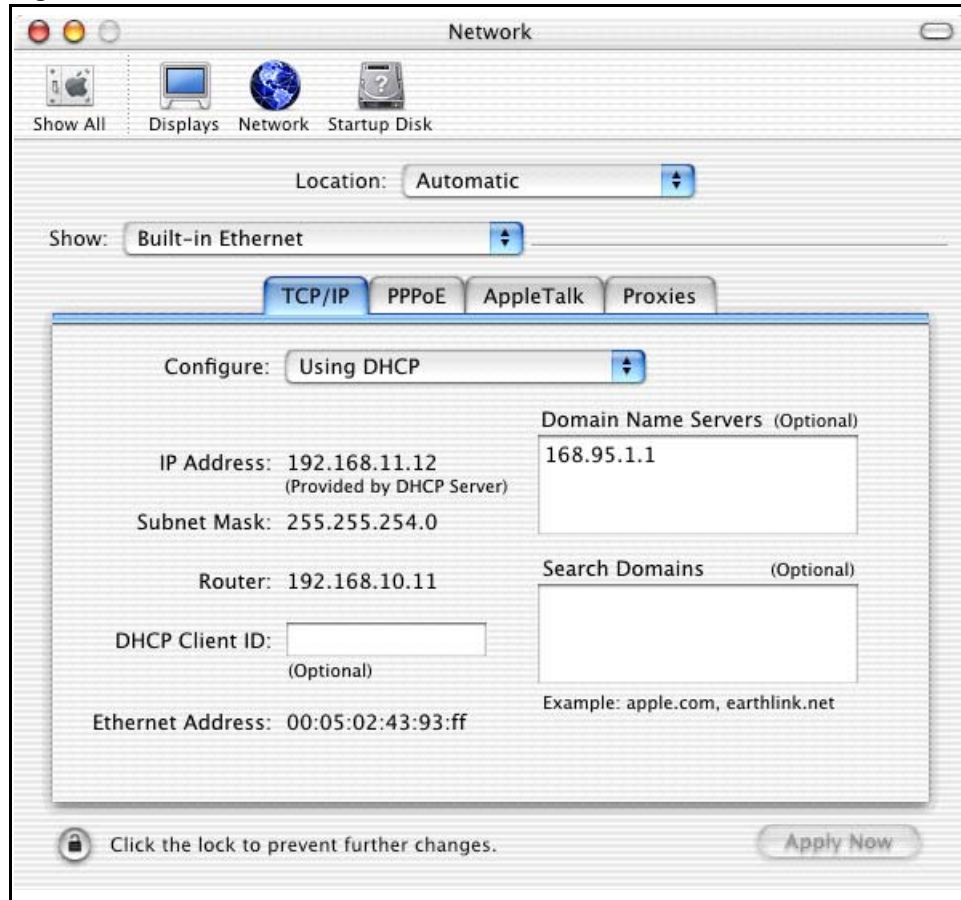
Macintosh OS X

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

Figure 123 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 124 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.

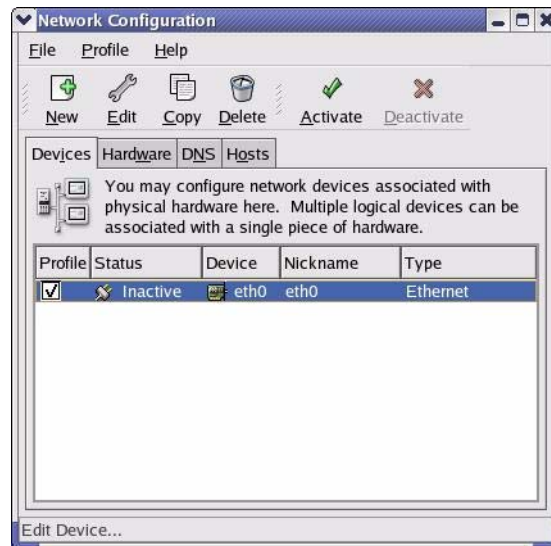
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

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

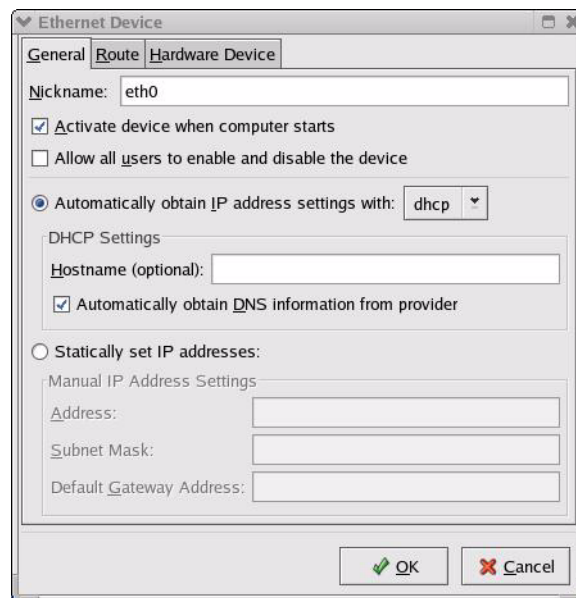
- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 125 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.

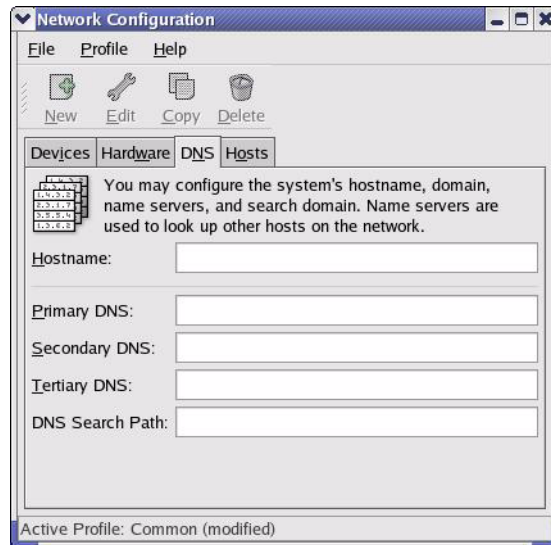
Figure 126 Red Hat 9.0: KDE: Ethernet Device: General



- 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.

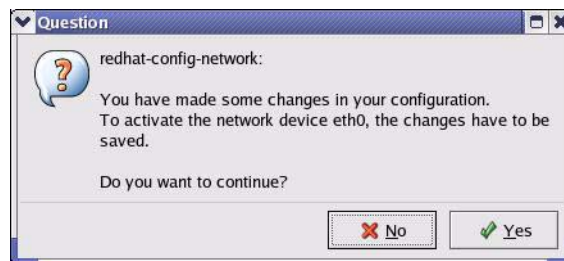
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.
- 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 127 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 128 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 129 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 130 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 131 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 132 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 133 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 D

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 75 Classes of IP Addresses

	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 76 Allowed IP Address Range By 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 77 “Natural” Masks

	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 78 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 78 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 79 Two Subnets Example

	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 80 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	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000

Table 80 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 81 Subnet 2

	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 82 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 82 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 83 Subnet 2

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

Table 84 Subnet 3

	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 85 Subnet 4

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

Example Eight Subnets

Similarly use a 27-bit mask to create 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 86 Eight Subnets

	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 87 Class C Subnet Planning

	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 75 on page 202](#)) available for subnetting.

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

Table 88 Class B Subnet Planning

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

Appendix E

Command Interpreter

The following describes how to use the command interpreter. See the included disk or 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.

Accessing the Command Interpreter

If your device has SMT, enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**.

If your device does not have SMT, simply Telnet to the ZyXEL Device's IP address. You will log directly into the command interpreter.

Command Syntax

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

For example,

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

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

Command Usage

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

APPENDIX F

Log Descriptions

This appendix provides descriptions of example log messages.

Table 89 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 89 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 90 System Error Logs

	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 91 Access Control Logs

	DESCRIPTION
Firewall default policy: [TCP UDP IGMP ESP GRE OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP UDP IGMP ESP GRE OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP UDP IGMP ESP GRE OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP UDP IGMP ESP GRE OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 92 TCP Reset Logs

	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to TCP Maximum Incomplete in the Firewall Attack Alerts screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.) Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: "sys firewall tcprst").

Table 93 Packet Filter Logs

	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 94 ICMP Logs

	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting. For type and code details, see Table 101 on page 217 .
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 101 on page 217 .
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

Table 95 CDR Logs

	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 96 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.

Table 96 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
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 97 UPnP Logs

	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 98 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: Keyword blocking	The content of a requested web page matched a user defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
%s:%s	The content filter server responded that the web site is in the blocked category list, and returned the category type.
%s (cache hit)	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
%s:%s (cache hit)	The system detected that the web site is in blocked list from the local cache, and knows the category type.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" check box, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The ZyXEL Device cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The ZyXEL Device cannot issue a query because TCP/IP socket creation failed, port:port number.

Table 98 Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

Table 99 Attack Logs

	DESCRIPTION
attack [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack. For type and code details, see Table 101 on page 217 .
land [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack. For type and code details, see Table 101 on page 217 .
ip spoofing - WAN [TCP UDP IGMP ESP GRE OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 101 on page 217 .
icmp echo: ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 101 on page 217 .
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack. For type and code details, see Table 101 on page 217 .
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP UDP IGMP ESP GRE OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 101 on page 217 .
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack. For type and code details, see Table 101 on page 217 .

Table 100 ACL Setting Notes

	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L/P)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W/P)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.

Table 101 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
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp

Table 101 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	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

Table 102 Syslog Logs

	DESCRIPTION
<pre><Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category></pre>	<p>"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.</p>

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 103 RFC-2408 ISAKMP Payload Types

	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Log Commands

This section provides some general examples of how to use the log commands. The items that display with your device may vary but the basic function should be the same.

Go to the command interpreter interface. [Appendix E on page 209](#) explains how to access and use the commands.

Configuring What You Want the ZyXEL Device to Log

- 1 Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.
- 2 Use `sys logs category` to view a list of the log categories.

Figure 134 Displaying Log Categories Example

```

Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
ras> sys logs category
access          attack          display         error
icmp            javablocked    mten           packetfilter
ppp             cdr            remote         tcpreset
traffic        upnp          urlblocked     urlforward
ras>

```

- 3 Use `sys logs category` followed by a log category to display the parameters that are available for the category.

Figure 135 Displaying Log Parameters Example

```

ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/
1:show debug type]

```

- 4 Use `sys logs category` followed by a log category and a parameter to decide what to record.
Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.
- 5 Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

Displaying Logs

- Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual ZyXEL Device log category.
- Use the `sys logs clear` command to erase all of the ZyXEL Device's logs.

Log Command Example

This example shows how to set the ZyXEL Device to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access
```

#.time	source	destination	notes
0	01/02/2000 04:06:35 192.168.1.33:2190	207.69.188.186:135	ACCESS
FORWARD Firewall default policy: TCP (L to W)			
1	01/02/2000 04:06:28 192.168.1.33:2190	207.69.188.186:135	ACCESS
FORWARD Firewall default policy: TCP (L to W)			
3	01/02/2000 04:06:25 192.168.1.33:2190	207.69.188.186:135	ACCESS
FORWARD Firewall default policy: UDP (L to W)			
4	01/02/2000 04:06:16 192.168.1.33:2187	207.69.188.186:80	ACCESS
FORWARD Firewall default policy: TCP (L to W)			

APPENDIX G

NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands.

Introduction

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

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

You can configure NetBIOS filters to do the following:

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

Display NetBIOS Filter Settings

```
sys filter netbios disp
```

This command gives a read-only list of the current NetBIOS filter modes for the ZyXEL Device.

NetBIOS Display Filter Settings Command Example

```
===== NetBIOS Filter Status =====  
Between LAN and WAN: Block  
IPSec Packets: Forward  
Trigger Dial: Disabled
```

The filter types and their default settings are as follows.

Table 104 NetBIOS Filter Default Settings

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

NetBIOS Filter Configuration

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

where

`<type>` = Identify which NetBIOS filter (numbered 0-3) to configure.

- 0 = Between LAN and WAN
- 3 = IPSec packet pass through
- 4 = Trigger Dial

`<on|off>` = For type 0 and 1, use on to enable the filter and block NetBIOS packets. Use off to disable the filter and forward NetBIOS packets. For type 3, use on to block NetBIOS packets from being sent through a VPN connection. Use off to allow NetBIOS packets to be sent through a VPN connection. For type 4, use on to allow NetBIOS packets to initiate dial backup calls. Use off to block NetBIOS packets from initiating dial backup calls.

Example commands

`sys filter netbios config 0 on` This command blocks LAN to WAN and WAN to LAN NetBIOS packets.

`sys filter netbios config 3 on` This command blocks IPSec NetBIOS packets.

`sys filter netbios config 4 off` This command stops NetBIOS commands from initiating calls.

APPENDIX H

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
 - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 105 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 105 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.

Table 105 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 105 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.

APPENDIX I

Wall-mounting Instructions

Do the following to hang your ZyXEL Device on a wall.

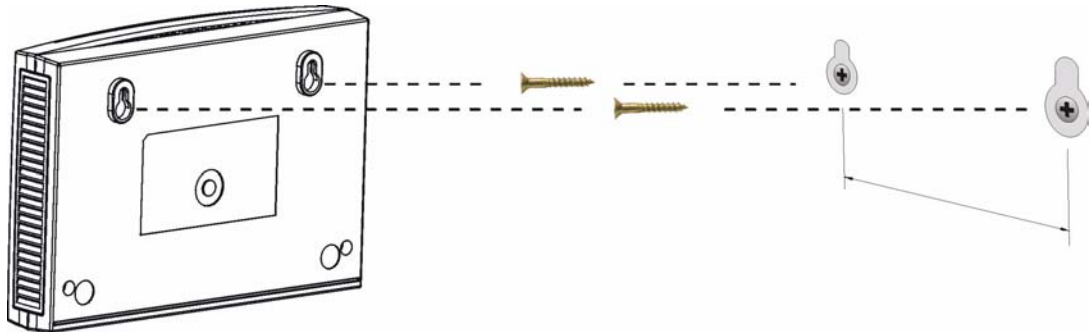
Note: See the product specifications appendix for the size of screws to use and how far apart to place them.

- 1 Locate a high position on wall that is free of obstructions. Use a sturdy wall.
- 2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

Note: Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyXEL Device with the connection cables.
- 5 Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

Figure 136 Wall-mounting Example



APPENDIX J

Internal SPTGEN

This appendix introduces Internal SPTGEN. All menus shown in this appendix are example menus meant to show SPTGEN usage. Actual menus for your product may differ.

Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple ZyXEL Devices. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to navigate and configure individual screens for each ZyXEL Device. You can use FTP to get the Internal SPTGEN file. Then edit the file in a text editor and use FTP to upload it again to the same device or another one. See the following sections for details.

The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

```
<field identification number = field name = parameter values
allowed = input>,
```

where <input> is your input conforming to <parameter values allowed>.

The figure shown next is an example of an Internal SPTGEN text file.

Figure 137 Configuration Text File Format: Column Descriptions

```
/ Menu 1 General Setup
10000000 = Configured          <0 (No) | 1 (Yes)>      = 1
10000001 = System Name        <Str>                  = Your Device
10000002 = Location           <Str>                  =
10000003 = Contact Person's Name <Str>                  =
10000004 = Route IP           <0 (No) | 1 (Yes)>      = 1
10000005 = Route IPX          <0 (No) | 1 (Yes)>      = 0
10000006 = Bridge             <0 (No) | 1 (Yes)>      = 0
```

Note: DO NOT alter or delete any field except parameters in the Input column.

This appendix introduces Internal SPTGEN. All menus shown in this appendix are example menus meant to show SPTGEN usage. Actual menus for your product may differ.

Internal SPTGEN File Modification - Important Points to Remember

Each parameter you enter must be preceded by one “=” sign and one space.

Some parameters are dependent on others. For example, if you disable the **Configured** field in menu 1 (see [Figure 137 on page 229](#)), then you disable every field in this menu.

If you enter a parameter that is invalid in the **Input** column, the ZyXEL Device will not save the configuration and the command line will display the **Field Identification Number**. [Figure 138 on page 230](#), shown next, is an example of what the ZyXEL Device displays if you enter a value other than “0” or “1” in the **Input** column of **Field Identification Number 1000000** (refer to [Figure 137 on page 229](#)).

Figure 138 Invalid Parameter Entered: Command Line Example

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

The ZyXEL Device will display the following if you enter parameter(s) that *are* valid.

Figure 139 Valid Parameter Entered: Command Line Example

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Internal SPTGEN FTP Download Example

- 1 Launch your FTP application.
- 2 Enter "bin". The command “bin” sets the transfer mode to binary.
- 3 Get "rom-t" file. The command “get” transfers files from the ZyXEL Device to your computer. The name “rom-t” is the configuration filename on the ZyXEL Device.
- 4 Edit the "rom-t" file using a text editor (do not use a word processor). You must leave this FTP screen to edit.

Figure 140 Internal SPTGEN FTP Download Example

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-t
ftp> bye
c:\edit rom-t
(edit the rom-t text file by a text editor and save it)
```

Note: You can rename your “rom-t” file when you save it to your computer but it must be named “rom-t” when you upload it to your ZyXEL Device.

Internal SPTGEN FTP Upload Example

- 1 Launch your FTP application.
- 2 Enter "bin". The command “bin” sets the transfer mode to binary.
- 3 Upload your “rom-t” file from your computer to the ZyXEL Device using the “put” command. computer to the ZyXEL Device.
- 4 Exit this FTP application.

Figure 141 Internal SPTGEN FTP Upload Example

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye
```

Example Internal SPTGEN Menus

This section provides example Internal SPTGEN menus.

Table 106 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number
FN	Field Name
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the ZyXEL Device.

Table 107 Menu 1 General Setup

/ Menu 1 General Setup			
FIN	FN	PVA	INPUT
10000000 =	Configured	<0 (No) 1 (Yes)>	= 0
10000001 =	System Name	<Str>	= Your Device
10000002 =	Location	<Str>	=
10000003 =	Contact Person's Name	<Str>	=
10000004 =	Route IP	<0 (No) 1 (Yes)>	= 1
10000006 =	Bridge	<0 (No) 1 (Yes)>	= 0

Table 108 Menu 3

/ Menu 3.1 General Ethernet Setup			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1		= 2
30100002 =	Input Protocol filters Set 2		= 256
30100003 =	Input Protocol filters Set 3		= 256
30100004 =	Input Protocol filters Set 4		= 256
30100005 =	Input device filters Set 1		= 256
30100006 =	Input device filters Set 2		= 256
30100007 =	Input device filters Set 3		= 256
30100008 =	Input device filters Set 4		= 256
30100009 =	Output protocol filters Set 1		= 256
30100010 =	Output protocol filters Set 2		= 256
30100011 =	Output protocol filters Set 3		= 256

Table 108 Menu 3

30100012 =	Output protocol filters Set 4		= 256
30100013 =	Output device filters Set 1		= 256
30100014 =	Output device filters Set 2		= 256
30100015 =	Output device filters Set 3		= 256
30100016 =	Output device filters Set 4		= 256
/ Menu 3.2 TCP/IP and DHCP Ethernet Setup			
FIN	FN	PVA	INPUT
30200001 =	DHCP	<0 (None) 1 (Server) 2 (Relay)>	= 0
30200002 =	Client IP Pool Starting Address		= 192.168.1.33
30200003 =	Size of Client IP Pool		= 32
30200004 =	Primary DNS Server		= 0.0.0.0
30200005 =	Secondary DNS Server		= 0.0.0.0
30200006 =	Remote DHCP Server		= 0.0.0.0
30200008 =	IP Address		= 172.21.2.200
30200009 =	IP Subnet Mask		= 16
30200010 =	RIP Direction	<0 (None) 1 (Both) 2 (In Only) 3 (Out Only)>	= 0
30200011 =	Version	<0 (Rip-1) 1 (Rip-2B) 2 (Rip-2M)>	= 0
30200012 =	Multicast	<0 (IGMP-v2) 1 (IGMP-v1) 2 (None)>	= 2
30200013 =	IP Policies Set 1 (1~12)		= 256
30200014 =	IP Policies Set 2 (1~12)		= 256
30200015 =	IP Policies Set 3 (1~12)		= 256
30200016 =	IP Policies Set 4 (1~12)		= 256
/ Menu 3.2.1 IP Alias Setup			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1	<0 (No) 1 (Yes)>	= 0
30201002 =	IP Address		= 0.0.0.0
30201003 =	IP Subnet Mask		= 0
30201004 =	RIP Direction	<0 (None) 1 (Both) 2 (In Only) 3 (Out Only)>	= 0

Table 108 Menu 3

30201005 =	Version	<0 (Rip-1) 1 (Rip-2B) 2 (Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2		= 256
30201008 =	IP Alias #1 Incoming protocol filters Set 3		= 256
30201009 =	IP Alias #1 Incoming protocol filters Set 4		= 256
30201010 =	IP Alias #1 Outgoing protocol filters Set 1		= 256
30201011 =	IP Alias #1 Outgoing protocol filters Set 2		= 256
30201012 =	IP Alias #1 Outgoing protocol filters Set 3		= 256
30201013 =	IP Alias #1 Outgoing protocol filters Set 4		= 256
30201014 =	IP Alias 2 <0 (No) 1 (Yes)>		= 0
30201015 =	IP Address		= 0.0.0.0
30201016 =	IP Subnet Mask		= 0
30201017 =	RIP Direction	<0 (None) 1 (Both) 2 (In Only) 3 (Out Only)>	= 0
30201018 =	Version	<0 (Rip-1) 1 (Rip-2B) 2 (Rip-2M)>	= 0
30201019 =	IP Alias #2 Incoming protocol filters Set 1		= 256
30201020 =	IP Alias #2 Incoming protocol filters Set 2		= 256
30201021 =	IP Alias #2 Incoming protocol filters Set 3		= 256
30201022 =	IP Alias #2 Incoming protocol filters Set 4		= 256
30201023 =	IP Alias #2 Outgoing protocol filters Set 1		= 256
30201024 =	IP Alias #2 Outgoing protocol filters Set 2		= 256
30201025 =	IP Alias #2 Outgoing protocol filters Set 3		= 256
30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256
*/ Menu 3.5 Wireless LAN Setup			

Table 108 Menu 3

FIN	FN	PVA	INPUT
30500001 =	ESSID		Wireless
30500002 =	Hide ESSID	<0 (No) 1 (Yes)>	= 0
30500003 =	Channel ID	<1 2 3 4 5 6 7 8 9 10 11 12 13>	= 1
30500004 =	RTS Threshold	<0 ~ 2432>	= 2432
30500005 =	FRAG. Threshold	<256 ~ 2432>	= 2432
30500006 =	WEP	<0 (DISABLE) 1 (64-bit WEP) 2 (128-bit WEP)>	= 0
30500007 =	Default Key	<1 2 3 4>	= 0
30500008 =	WEP Key1		=
30500009 =	WEP Key2		=
30500010 =	WEP Key3		=
30500011 =	WEP Key4		=
30500012 =	Wlan Active	<0 (Disable) 1 (Enable)>	= 0
30500013 =	Wlan 4X Mode	<0 (Disable) 1 (Enable)>	= 0
*/ MENU 3.5.1 WLAN MAC ADDRESS FILTER			
FIN	FN	PVA	INPUT
30501001 =	Mac Filter Active	<0 (No) 1 (Yes)>	= 0
30501002 =	Filter Action	<0 (Allow) 1 (Deny)>	= 0
30501003 =	Address 1		= 00:00:00:00:0 0:00
30501004 =	Address 2		= 00:00:00:00:0 0:00
30501005 =	Address 3		= 00:00:00:00:0 0:00
Continued
30501034 =	Address 32		= 00:00:00:00:0 0:00

Table 109 Menu 4 Internet Access Setup

/ Menu 4 Internet Access Setup			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0 (No) 1 (Yes)>	= 1
40000001 =	ISP	<0 (No) 1 (Yes)>	= 1
40000002 =	Active	<0 (No) 1 (Yes)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2 (PPPOE) 3 (RFC 1483) 4 (PPPoA) 5 (ENET ENCAP)>	= 2
40000005 =	Multiplexing	<1 (LLC-based) 2 (VC-based)>	= 1
40000006 =	VPI #		= 0
40000007 =	VCI #		= 35
40000008 =	Service Name	<Str>	= any
40000009 =	My Login	<Str>	= test@pqa
40000010 =	My Password	<Str>	= 1234
40000011 =	Single User Account	<0 (No) 1 (Yes)>	= 1
40000012 =	IP Address Assignment	<0 (Static) 1 (Dynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0 (No) 1 (Yes)>	= 1
40000026 =	Bridge	<0 (No) 1 (Yes)>	= 0

Table 109 Menu 4 Internet Access Setup (continued)

40000027 =	ATM QoS Type	<0 (CBR) 1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR)		= 0
40000029 =	Sustain Cell Rate (SCR)		= 0
40000030 =	Maximum Burst Size (MBS)		= 0
40000031=	RIP Direction	<0 (None) 1 (Both) 2 (In Only) 3 (Out Only)>	= 0
40000032=	RIP Version	<0 (Rip-1) 1 (Rip-2B) 2 (Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0 (No) 1 (Yes)>	= 0

Table 110 Menu 12

/ Menu 12.1.1 IP Static Route Setup			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0 (No) 1 (Yes)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0 (No) 1 (Yes)>	= 0
/ Menu 12.1.2 IP Static Route Setup			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name	<Str>	=
120108002 =	IP Static Route set #8, Active	<0 (No) 1 (Yes)>	= 0
120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0
120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0 (No) 1 (Yes)>	= 0

Table 111 Menu 15 SUA Server Setup

/ Menu 15 SUA Server Setup			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Active	<0 (No) 1 (Yes)>	= 0
150000003 =	SUA Server #2 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000004 =	SUA Server #2 Port Start		= 0
150000005 =	SUA Server #2 Port End		= 0
150000006 =	SUA Server #2 Local IP address		= 0.0.0.0
150000007 =	SUA Server #3 Active	<0 (No) 1 (Yes)>	= 0
150000008 =	SUA Server #3 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000009 =	SUA Server #3 Port Start		= 0
150000010 =	SUA Server #3 Port End		= 0
150000011 =	SUA Server #3 Local IP address		= 0.0.0.0
150000012 =	SUA Server #4 Active	<0 (No) 1 (Yes)>	= 0
150000013 =	SUA Server #4 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0 (No) 1 (Yes)>	= 0
150000018 =	SUA Server #5 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000019 =	SUA Server #5 Port Start		= 0
150000020 =	SUA Server #5 Port End		= 0
150000021 =	SUA Server #5 Local IP address		= 0.0.0.0
150000022 =	SUA Server #6 Active	<0 (No) 1 (Yes)> = 0	= 0
150000023 =	SUA Server #6 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000024 =	SUA Server #6 Port Start		= 0
150000025 =	SUA Server #6 Port End		= 0
150000026 =	SUA Server #6 Local IP address		= 0.0.0.0
150000027 =	SUA Server #7 Active	<0 (No) 1 (Yes)>	= 0
150000028 =	SUA Server #7 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0

Table 111 Menu 15 SUA Server Setup (continued)

150000031 =	SUA Server #7 Local IP address		= 0.0.0.0
150000032 =	SUA Server #8 Active	<0 (No) 1 (Yes)>	= 0
150000033 =	SUA Server #8 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000034 =	SUA Server #8 Port Start		= 0
150000035 =	SUA Server #8 Port End		= 0
150000036 =	SUA Server #8 Local IP address		= 0.0.0.0
150000037 =	SUA Server #9 Active	<0 (No) 1 (Yes)>	= 0
150000038 =	SUA Server #9 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000039 =	SUA Server #9 Port Start		= 0
150000040 =	SUA Server #9 Port End		= 0
150000041 =	SUA Server #9 Local IP address		= 0.0.0.0
150000042 =	SUA Server #10 Active	<0 (No) 1 (Yes)>	= 0
150000043 =	SUA Server #10 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000044 =	SUA Server #10 Port Start		= 0
150000045 =	SUA Server #10 Port End		= 0
150000046 =	SUA Server #10 Local IP address		= 0.0.0.0
150000047 =	SUA Server #11 Active	<0 (No) 1 (Yes)>	= 0
150000048 =	SUA Server #11 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000049 =	SUA Server #11 Port Start		= 0
150000050 =	SUA Server #11 Port End		= 0
150000051 =	SUA Server #11 Local IP address		= 0.0.0.0
150000052 =	SUA Server #12 Active	<0 (No) 1 (Yes)>	= 0
150000053 =	SUA Server #12 Protocol	<0 (All) 6 (TCP) 17 (UDP)>	= 0
150000054 =	SUA Server #12 Port Start		= 0
150000055 =	SUA Server #12 Port End		= 0
150000056 =	SUA Server #12 Local IP address		= 0.0.0.0

Table 112 Menu 21.1 Filter Set #1

/ Menu 21 Filter set #1			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=
/ Menu 21.1.1.1 set #1, rule #1			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1, Rule 1 Type	<2 (TCP/IP)>	= 2

Table 112 Menu 21.1 Filter Set #1 (continued)

210101002 =	IP Filter Set 1,Rule 1 Active	<0 (No) 1 (Yes)>	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address		= 0.0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask		= 0
210101006 =	IP Filter Set 1,Rule 1 Dest Port		= 137
210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match	<1 (check next) 2 (forward) 3 (drop)>	= 1
/ Menu 21.1.1.2 set #1, rule #2			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type	<2 (TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0 (No) 1 (Yes)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210102008 =	IP Filter Set 1,Rule 2 Src IP address		= 0.0.0.0
210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port		= 0
210102011 =	IP Filter Set 1,Rule 2 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0

Table 112 Menu 21.1 Filter Set #1 (continued)

210102013 =	IP Filter Set 1,Rule 2 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match	<1 (check next) 2 (forward) 3 (drop)>	= 1

Table 113 Menu 21.1 Filer Set #2,

/ Menu 21.1 filter set #2,			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN
/ Menu 21.1.2.1 Filter set #2, rule #1			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2, Rule 1 Type	<0 (none) 2 (TCP/IP)>	= 2
210201002 =	IP Filter Set 2, Rule 1 Active	<0 (No) 1 (Yes)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port		= 137
210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210201008 =	IP Filter Set 2, Rule 1 Src IP address		= 0.0.0.0
210201009 =	IP Filter Set 2, Rule 1 Src Subnet Mask		= 0
210201010 =	IP Filter Set 2, Rule 1 Src Port		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210201014 =	IP Filter Set 2, Rule 1 Act Not Match	<1 (check next) 2 (forward) 3 (drop)>	= 1
/ Menu 21.1.2.2 Filter set #2, rule #2			
FIN	FN	PVA	INPUT

Table 113 Menu 21.1 Filer Set #2, (continued)

210202001 =	IP Filter Set 2, Rule 2 Type	<0 (none) 2 (TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active	<0 (No) 1 (Yes)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address		= 0.0.0.0
210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask		= 0
210202010 =	IP Filter Set 2, Rule 2 Src Port		= 0
210202011 =	IP Filter Set 2, Rule 2 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210202014 =	IP Filter Set 2, Rule 2 Act Not Match	<1 (check next) 2 (forward) 3 (drop)>	= 1

Table 114 Menu 23 System Menus

*/ Menu 23.1 System Password Setup			
FIN	FN	PVA	INPUT
230000000 =	System Password		= 1234
*/ Menu 23.2 System security: radius server			
FIN	FN	PVA	INPUT
230200001 =	Authentication Server Configured	<0 (No) 1 (Yes)>	= 1
230200002 =	Authentication Server Active	<0 (No) 1 (Yes)>	= 1
230200003 =	Authentication Server IP Address		= 192.168.1.32
230200004 =	Authentication Server Port		= 1822

Table 114 Menu 23 System Menus (continued)

230200005 =	Authentication Server Shared Secret		= 111111111111 111 111111111111 1111
230200006 =	Accounting Server Configured	<0 (No) 1 (Yes)>	= 1
230200007 =	Accounting Server Active	<0 (No) 1 (Yes)>	= 1
230200008 =	Accounting Server IP Address		= 192.168.1.44
230200009 =	Accounting Server Port		= 1823
230200010 =	Accounting Server Shared Secret		= 1234
*/ Menu 23.4 System security: IEEE802.1x			
FIN	FN	PVA	INPUT
230400001 =	Wireless Port Control	<0 (Authentication Required) 1 (No Access Allowed) 2 (No Authentication Required)>	= 2
230400002 =	ReAuthentication Timer (in second)		= 555
230400003 =	Idle Timeout (in second)		= 999
230400004 =	Authentication Databases	<0 (Local User Database Only) 1 (RADIUS Only) 2 (Local, RADIUS) 3 (RADIUS, Local)>	= 1
230400005 =	Key Management Protocol	<0 (8021x) 1 (WPA) 2 (WPA2)>	= 0
230400006 =	Dynamic WEP Key Exchange	<0 (Disable) 1 (64-bit WEP) 2 (128-bit WEP)>	= 0
230400007 =	PSK =		=
230400008 =	WPA Mixed Mode	<0 (Disable) 1 (Enable)>	= 0
230400009 =	Data Privacy for Broadcast/Multicast packets	<0 (TKIP) 1 (WEP)>	= 0
230400010 =	WPA Broadcast/Multicast Key Update Timer		= 0

Table 115 Menu 24.11 Remote Management Control

/ Menu 24.11 Remote Management Control			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port		= 23

Table 115 Menu 24.11 Remote Management Control (continued)

241100002 =	TELNET Server Access	<0 (all) 1 (none) 2 (Lan) 3 (Wan) >	= 0
241100003 =	TELNET Server Secured IP address		= 0.0.0.0
241100004 =	FTP Server Port		= 21
241100005 =	FTP Server Access	<0 (all) 1 (none) 2 (Lan) 3 (Wan) >	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0 (all) 1 (none) 2 (Lan) 3 (Wan) >	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

Command Examples

The following are example Internal SPTGEN screens associated with the ZyXEL Device's command interpreter commands.

Table 116 Command Examples

	FN	PVA	INPUT
/ci command (for annex a): wan adsl opencmd			
	FN	PVA	INPUT
	ADSL OPMD	<0 (glite) 1 (t1.413) 2 (gdm) 3 (multimode) >	= 3
/ci command (for annex B): wan adsl opencmd			
	FN	PVA	INPUT
	ADSL OPMD	<0 (etsi) 1 (normal) 2 (gdm) 3 (multimode) >	= 3

Index

A

- ActiveX [96](#)
- alternative subnet mask notation [203](#)
- Applications [27, 28](#)
 - PR switch [27](#)
 - Print Server [27](#)
 - Print Server and Router combined [28](#)
 - USB port [27](#)
- Asymmetrical routes [90](#)
 - and IP alias [91](#)
 - see also triangle routes [90](#)

B

- Backup [157](#)
- Bandwidth Management [105](#)
 - Application-based [105](#)
 - Classes [110](#)
 - Classes and priorities [110](#)
 - Monitor [116](#)
 - Priority [107](#)
 - Services [107](#)
 - Subnet-based [105](#)
- Bandwidth management monitor [116](#)

C

- Certifications
 - Notice 1 [4](#)
 - viewing [4](#)
- Configuration [156](#)
 - Backup [157](#)
 - reset the factory defaults [158](#)
 - Restore [157](#)
- Contact Information [7](#)
- Content Filtering [95](#)
 - Days and Times [95](#)
 - Restrict Web Features [95](#)
- Cookies [96](#)

- Copyright [3](#)
- Customer Support [7](#)

D

- DDNS [87](#)
 - see also Dynamic DNS
- Default [158](#)
- DHCP [40, 73](#)
 - DHCP server
 - See also Dynamic Host Configuration Protocol
- DHCP table [40, 75](#)
 - DHCP client information
 - DHCP status
- DHCP Table Summary [40](#)
- DHCP_client list [75](#)
- Disclaimer [3](#)
- DNS [51, 121](#)
 - DNS server
 - see also Domain name system
- Domain name [45](#)
 - vs host name. see also system name
- Dynamic DNS [87](#)
- Dynamic Host Configuration Protocol [73](#)
 - DHCP server
 - see also DHCP

F

- Factory LAN Defaults [67](#)
- FCC [4](#)
- Federal Communications Commission [4](#)
- Firewall [89](#)
 - Firewall overview
 - ICMP packets [92](#)
 - network security
 - Stateful inspection [89](#)
 - ZyXEL device firewall [89](#)
- Firmware upload [155](#)
 - file extension

using HTTP
FTP [117](#), [120](#)
FTP Restrictions [117](#)

H

Host [148](#)

I

IGMP [68](#)
Interference Statement [4](#)
Internal SPTGEN [229](#)
 FTP Upload Example [231](#)
 Points to Remember [230](#)
 Text File [229](#)
Internet Access Setup [164](#)
Internet connection [45](#)
 Ethernet
 PPPoE. see also PPP over Ethernet
 PPTP
 WAN connection
IP Address [40](#), [68](#), [69](#), [75](#), [79](#)
IP address [51](#)
 dynamic
IP address assignment [50](#)
IP alias [69](#)
IP packet transmission [68](#)
 Broadcast
 Multicast
 Unicast
IP Pool [73](#)
IP Pool Setup [67](#)

J

Java [96](#)

L

LAN [67](#)
 see also Local Area Network
LAN parameters [67](#)
 DHCP server

IP address
LAN Setup [67](#)
LAN TCP/IP [67](#)
Logs [151](#)

M

MAC [53](#)
 MAC address
 see also Media Access Control
MAC address [57](#)
MAC address cloning [53](#)
Media Access Control [74](#)
 MAC address
 see also MAC
Metric [103](#)
Multicast [66](#), [68](#), [70](#)
 IGMP version
 IGMP. see also Internet Group Multicast Protocol

N

NAT [77](#)
 see also Network Address Translation
Navigation Panel [37](#)
Navigation panel [37](#)
NetBIOS [66](#)
 see also Network Basic Input/Output System

P

Packet statistics [40](#)
Point-to-Point Protocol over Ethernet [59](#)
Point-to-Point Tunneling Protocol [62](#)
Port forwarding
 default server [77](#)
 local server [79](#)
port forwarding [77](#)
 inside server
Port Forwarding Example [78](#)
port forwarding set [77](#)
Port number [77](#)
port number
 and port forwarding
 vs services
PPPoE [47](#), [59](#)

dial-up connection
 see also Point-to-Point Protocol over Ethernet [47](#)
 PPTP [48, 62](#)
 see also Point-to-Point Tunneling Protocol [48](#)
 Print server [131](#)
 driver installation requirements [133](#)
 Print server driver [131](#)
 Private [103](#)

R

Related Documentation [25](#)
 Remote management [117](#)
 and firewall [117](#)
 and NAT [118](#)
 FTP [120](#)
 Limitations [117](#)
 remote management session [117](#)
 system timeout [118](#)
 Telnet [119](#)
 Reset button [32](#)
 Reset the device [32](#)
 Restore [157](#)
 Restrict Web Features [96](#)

S

Safety Warnings [5](#)
 Service and port numbers [108](#)
 Service Type [164](#)
 Services [92](#)
 SNMP [90](#)
 Static DHCP [74](#)
 Static Route [101](#)
 Static route
 and remote node
 overview
 Status [32, 35](#)
 Print server mode
 Router mode [32](#)
 subnet [201](#)
 Subnet Mask [68, 69](#)
 Subnet mask [51](#)
 subnet mask [203](#)
 subnetting [203](#)
 Summary [39](#)
 Bandwidth management monitor [39](#)
 DHCP table [40](#)
 Packet statistics [40](#)

Syntax Conventions [25](#)
 System General Setup [147](#)
 System information [44](#)
 System Maintenance [152](#)
 System Name [44](#)
 System name [148](#)
 System Parameter Table Generator [229](#)
 System restart [159](#)
 System Timeout [118](#)

T

TCP/IP [69](#)
 Text File Format [229](#)
 TFTP Restrictions [117](#)
 Time Zone [148](#)
 Trademarks [3](#)
 Triangle routes
 and IP alias [91](#)
 see also asymmetrical routes [90](#)
 Trigger port forwarding [82](#)
 incoming port
 trigger port
 Trigger port forwarding example [83](#)

U

Universal Plug and Play [123](#)
 UPnP [123](#)
 cautions with UPnP [123](#)
 Forum [124](#)
 how to install UPnP [125](#)
 see also Universal Plug and Play
 UPnP and ZyXEL [124](#)
 vs NAT traversal [123](#)
 URL Keyword Blocking [96](#)
 User Name [88](#)

V

VPN [62](#)
 vs computer name

W

- WAN advanced [65](#)
- WAN IP address assignment [51](#)
- WAN MAC address [53](#)
- WAN Wizard [45](#)
- Warnings [5](#)
- Web [118](#)
- Web Configurator [32](#)
 - how to access [31](#)
 - Introduction [31](#)
 - navigating [32](#)
 - Overview [31](#)
- Web Proxy [96](#)
- Wildcard [87](#)
- Wizard setup [43](#)

Z

- ZyXEL Limited Warranty
 - Note [6](#)