

P-2602R/RL-DxA Series

ADSL2+ VoIP IAD

User's Guide

Version 3.40

6/2006

Edition 1

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Z" and "y" are lowercase, while "XEL" are 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.

Certifications

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



Safety Warnings

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

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- Do not use the device outside, and make sure all the connections are indoors. There may be a remote risk of electric shock from lightning.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

ZyXEL Limited Warranty

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

Note

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

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

Customer Support

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

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

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

METHOD	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
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	

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

Table of Contents

Copyright	3
Certifications	4
Safety Warnings	6
ZyXEL Limited Warranty	7
Customer Support	8
Table of Contents	11
List of Figures	23
List of Tables	29
Preface	33
Chapter 1	
Getting To Know the ZyXEL Device	35
1.1 Introducing the P-2602RL-DxA Series	35
1.2 Features	36
1.3 Applications for the ZyXEL Device	40
1.3.1 Internet Access	40
1.3.1.1 Internet Single User Account	40
1.3.2 Making Calls via Internet Telephony Service Provider	40
1.3.3 Make Peer-to-peer Calls	41
1.3.4 Firewall for Secure Broadband Internet Access	41
1.3.5 LEDs	42
Chapter 2	
Introducing the Web Configurator	45
2.1 Web Configurator Overview	45
2.1.1 Accessing the Web Configurator	45
2.1.2 The RESET Button	47
2.1.2.1 Using The Reset Button	47
2.2 Web Configurator Main Screen	48
2.2.1 Title Bar	48
2.2.2 Navigation Panel	49
2.2.3 Main Window	51
2.2.4 Status Bar	51

Chapter 3	
Internet Setup Wizard	53
3.1 Introduction	53
3.2 Internet Access Wizard Setup	53
3.2.1 Manual Configuration	55
Chapter 4	
VoIP Wizard And Example	61
4.1 Introduction	61
4.2 VoIP Wizard Setup	61
Chapter 5	
Bandwidth Management Wizard	67
5.1 Introduction	67
5.2 Predefined Media Bandwidth Management Services	67
5.3 Bandwidth Management Wizard Setup	68
Chapter 6	
Status Screens	73
6.1 Status Screen	73
6.2 Any IP Table	76
6.3 Packet Statistics	77
6.4 VoIP Statistics	78
Chapter 7	
WAN Setup	81
7.1 WAN Overview	81
7.1.1 Encapsulation	81
7.1.1.1 ENET ENCAP	81
7.1.1.2 PPP over Ethernet	81
7.1.1.3 PPPoA	82
7.1.1.4 RFC 1483	82
7.1.2 Multiplexing	82
7.1.2.1 VC-based Multiplexing	82
7.1.2.2 LLC-based Multiplexing	82
7.1.3 VPI and VCI	82
7.1.4 IP Address Assignment	83
7.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation	83
7.1.4.2 IP Assignment with RFC 1483 Encapsulation	83
7.1.4.3 IP Assignment with ENET ENCAP Encapsulation	83
7.1.5 Nailed-Up Connection (PPP)	83
7.1.6 NAT	83
7.2 Metric	84

7.3 Traffic Shaping	84
7.3.1 ATM Traffic Classes	85
7.3.1.1 Constant Bit Rate (CBR)	85
7.3.1.2 Variable Bit Rate (VBR)	85
7.3.1.3 Unspecified Bit Rate (UBR)	86
7.4 Zero Configuration Internet Access	86
7.5 Internet Access Setup	86
7.5.1 Advanced Internet Access Setup.....	89
7.6 WAN More Connections	90
7.7 Traffic Redirect	91
7.8 WAN Backup Setup	93
Chapter 8	
LAN Setup.....	95
8.1 LAN Overview	95
8.1.1 LANs, WANs and the ZyXEL Device	95
8.1.2 DHCP Setup	96
8.1.2.1 IP Pool Setup	96
8.1.3 DNS Server Address	96
8.1.4 DNS Server Address Assignment	97
8.2 LAN TCP/IP	97
8.2.1 IP Address and Subnet Mask	97
8.2.1.1 Private IP Addresses	98
8.2.2 RIP Setup	98
8.2.3 Multicast	99
8.2.4 Any IP	99
8.2.4.1 How Any IP Works	100
8.3 Configuring LAN IP	101
8.3.1 Configuring Advanced LAN Setup.....	101
8.4 DHCP Setup	103
8.5 LAN Client List	104
8.6 LAN IP Alias	106
Chapter 9	
Network Address Translation (NAT) Screens	109
9.1 NAT Overview	109
9.1.1 NAT Definitions	109
9.1.2 What NAT Does	110
9.1.3 How NAT Works	110
9.1.4 NAT Application	111
9.1.5 NAT Mapping Types	111
9.2 SUA (Single User Account) Versus NAT	112
9.3 NAT General Setup	112

9.4 Port Forwarding	113
9.4.1 Default Server IP Address	114
9.4.2 Port Forwarding: Services and Port Numbers	114
9.4.3 Configuring Servers Behind Port Forwarding (Example)	115
9.5 Configuring Port Forwarding	115
9.5.1 Port Forwarding Rule Edit	116
9.5.2 SIP ALG	117
Chapter 10	
Voice	119
10.1 Introduction to VoIP	119
10.2 SIP	119
10.2.1 SIP Identities	119
10.2.1.1 SIP Number	119
10.2.1.2 SIP Service Domain	120
10.2.2 SIP Call Progression	120
10.2.3 SIP Servers	120
10.2.3.1 SIP User Agent	121
10.2.3.2 SIP Proxy Server	121
10.2.3.3 SIP Redirect Server	122
10.2.3.4 SIP Register Server	123
10.2.3.5 Multiple SIP Accounts	123
10.3 SIP Settings Screen	123
10.3.1 RTP	125
10.4 Pulse Code Modulation	125
10.5 Voice Coding	125
10.5.1 G.711	125
10.5.2 G.729	125
10.6 PSTN Call Setup Signaling	126
10.7 MWI (Message Waiting Indication)	126
10.8 Custom Tones (IVR)	126
10.8.0.1 Recording Custom Tones	126
10.8.0.2 Listening to Custom Tones	127
10.8.0.3 Deleting Custom Tones	127
10.9 Advanced SIP Setup Screen	127
10.10 Quality of Service (QoS)	131
10.10.1 Type Of Service (ToS)	131
10.10.2 DiffServ	131
10.10.2.1 DSCP and Per-Hop Behavior	131
10.10.3 VLAN	132
10.10.4 SIP QoS Screen	132
10.11 Phone	133
10.11.1 PSTN Line ("L" Models only)	133

10.11.2 Voice Activity Detection/Silence Suppression	133
10.11.3 Comfort Noise Generation	133
10.11.4 Echo Cancellation	134
10.12 Analog Phone	134
10.13 Advanced Analog Phone Setup Screen	135
10.13.1 Common Phone Settings Screen	136
10.14 Supplementary Phone Services Overview	137
10.14.1 The Flash Key	138
10.14.2 Europe Type Supplementary Phone Services	138
10.14.2.1 European Call Hold	138
10.14.2.2 European Call Waiting	139
10.14.2.3 European Call Transfer	139
10.14.2.4 European Three-Way Conference	139
10.14.3 USA Type Supplementary Services	139
10.14.3.1 USA Call Hold	140
10.14.3.2 USA Call Waiting	140
10.14.3.3 USA Call Transfer	140
10.14.3.4 USA Three-Way Conference	140
10.15 Phone Region Screen	141
10.16 Speed Dial	141
10.16.1 Peer-to-Peer Calls	142
10.17 Speed Dial Screen	142
10.18 Incoming Call Policy Screen	143
10.19 PSTN Line Screen	145
Chapter 11	
Phone Usage	147
11.1 Dialing a Telephone Number	147
11.2 Using Speed Dial to Dial a Telephone Number	147
11.3 Internal Calls	147
11.4 Checking the Device's IP Address	147
11.5 Auto Firmware Upgrade	148
Chapter 12	
Firewalls	149
12.1 Firewall Overview	149
12.2 Types of Firewalls	149
12.2.1 Packet Filtering Firewalls	149
12.2.2 Application-level Firewalls	150
12.2.3 Stateful Inspection Firewalls	150
12.3 Introduction to ZyXEL's Firewall	150
12.3.1 Denial of Service Attacks	151
12.4 Denial of Service	151

12.4.1 Basics	151
12.4.2 Types of DoS Attacks	152
12.4.2.1 ICMP Vulnerability	154
12.4.2.2 Illegal Commands (NetBIOS and SMTP)	154
12.4.2.3 Traceroute	155
12.5 Stateful Inspection	155
12.5.1 Stateful Inspection Process	156
12.5.2 Stateful Inspection on Your ZyXEL Device	156
12.5.3 TCP Security	157
12.5.4 UDP/ICMP Security	157
12.5.5 Upper Layer Protocols	158
12.6 Guidelines for Enhancing Security with Your Firewall	158
12.6.1 Security In General	158
12.7 Packet Filtering Vs Firewall	159
12.7.1 Packet Filtering:	159
12.7.1.1 When To Use Filtering	160
12.7.2 Firewall	160
12.7.2.1 When To Use The Firewall	160
Chapter 13	
Firewall Configuration	161
13.1 Access Methods	161
13.2 Firewall Policies Overview	161
13.3 Rule Logic Overview	162
13.3.1 Rule Checklist	162
13.3.2 Security Ramifications	162
13.3.3 Key Fields For Configuring Rules	163
13.3.3.1 Action	163
13.3.3.2 Service	163
13.3.3.3 Source Address	163
13.3.3.4 Destination Address	163
13.4 Connection Direction	163
13.4.1 LAN to WAN Rules	164
13.4.2 Alerts	164
13.5 General Firewall Policy	164
13.6 Firewall Rules Summary	165
13.6.1 Configuring Firewall Rules	167
13.6.2 Customized Services	170
13.6.3 Configuring A Customized Service	171
13.7 Example Firewall Rule	171
13.8 DoS Thresholds	175
13.8.1 Threshold Values	175
13.8.2 Half-Open Sessions	176

13.8.2.1 TCP Maximum Incomplete and Blocking Time	176
13.8.3 Configuring Firewall Thresholds	177
Chapter 14	
Content Filtering	179
14.1 Content Filtering Overview	179
14.2 Configuring Keyword Blocking	179
14.3 Configuring the Schedule	180
14.4 Configuring Trusted Computers	181
Chapter 15	
Static Route	183
15.1 Static Route	183
15.2 Configuring Static Route	183
15.2.1 Static Route Edit	185
Chapter 16	
Bandwidth Management	187
16.1 Bandwidth Management Overview	187
16.2 Application-based Bandwidth Management	187
16.3 Subnet-based Bandwidth Management	187
16.4 Application and Subnet-based Bandwidth Management	188
16.5 Scheduler	188
16.5.1 Priority-based Scheduler	188
16.5.2 Fairness-based Scheduler	188
16.6 Maximize Bandwidth Usage	189
16.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic	189
16.6.2 Maximize Bandwidth Usage Example	189
16.6.2.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth	190
16.6.2.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth	190
16.6.3 Bandwidth Management Priorities	191
16.7 Configuring Summary	191
16.8 Bandwidth Management Rule Setup	192
16.8.1 Rule Configuration	194
16.9 Bandwidth Monitor	196
Chapter 17	
Dynamic DNS Setup.....	197
17.1 Dynamic DNS Overview	197
17.1.1 DYNDNS Wildcard	197
17.2 Configuring Dynamic DNS	197

Chapter 18	
Remote Management Configuration	201
18.1 Remote Management Overview	201
18.1.1 Remote Management Limitations	201
18.1.2 Remote Management and NAT	202
18.1.3 System Timeout	202
18.2 WWW	202
18.3 Telnet	203
18.4 Configuring Telnet	203
18.5 Configuring FTP	204
18.6 SNMP	205
18.6.1 Supported MIBs	207
18.6.2 SNMP Traps	207
18.6.3 Configuring SNMP	207
18.7 Configuring DNS	209
18.8 Configuring ICMP	209
Chapter 19	
Universal Plug-and-Play (UPnP)	211
19.1 Introducing Universal Plug and Play	211
19.1.1 How do I know if I'm using UPnP?	211
19.1.2 NAT Traversal	211
19.1.3 Cautions with UPnP	212
19.2 UPnP and ZyXEL	212
19.2.1 Configuring UPnP	212
19.3 Installing UPnP in Windows Example	213
19.4 Using UPnP in Windows XP Example	216
Chapter 20	
System	223
20.1 General Setup and System Name	223
20.1.1 General Setup	223
20.2 Time Setting	225
Chapter 21	
Logs	229
21.1 Logs Overview	229
21.1.1 Alerts and Logs	229
21.2 Viewing the Logs	229
21.3 Configuring Log Settings	230
21.4 SMTP Error Messages	233
21.4.1 Example E-mail Log	233

Chapter 22	
Tools	235
22.1 Introduction	235
22.2 Filename Conventions	235
22.3 File Maintenance Over WAN	236
22.4 Firmware Upgrade Screen	236
22.5 Backup and Restore	238
22.5.1 Backup Configuration	239
22.5.2 Restore Configuration	239
22.5.3 Reset to Factory Defaults	240
22.6 Restart	241
22.7 Using FTP or TFTP to Back Up Configuration	241
22.7.1 Using the FTP Commands to Back Up Configuration	241
22.7.2 FTP Command Configuration Backup Example	242
22.7.3 Configuration Backup Using GUI-based FTP Clients	242
22.7.4 Backup Configuration Using TFTP	243
22.7.5 TFTP Command Configuration Backup Example	243
22.7.6 Configuration Backup Using GUI-based TFTP Clients	244
22.8 Using FTP or TFTP to Restore Configuration	244
22.8.1 Restore Using FTP Session Example	245
22.9 FTP and TFTP Firmware and Configuration File Uploads	245
22.9.1 FTP File Upload Command from the DOS Prompt Example	245
22.9.2 FTP Session Example of Firmware File Upload	246
22.9.3 TFTP File Upload	246
22.9.4 TFTP Upload Command Example	247
Chapter 23	
Diagnostic	249
23.1 General Diagnostic	249
23.2 DSL Line Diagnostic	249
Chapter 24	
Troubleshooting	253
24.1 Problems Starting Up the ZyXEL Device	253
24.2 Problems with the LAN	253
24.3 Problems with the WAN	254
24.4 Problems Accessing the ZyXEL Device	255
24.4.1 Pop-up Windows, JavaScripts and Java Permissions	255
24.4.1.1 Internet Explorer Pop-up Blockers	256
24.4.1.2 JavaScripts	259
24.4.1.3 Java Permissions	261
24.5 Telephone Problems	263
24.6 Problems With Multiple SIP Accounts	264

24.6.1 Outgoing Calls	264
24.6.2 Incoming Calls	265
Appendix A	
Product Specifications	267
Appendix B	
Splitters and Microfilters	271
Connecting a POTS Splitter	271
Telephone Microfilters	271
Appendix C	
Setting up Your Computer's IP Address.....	273
Windows 95/98/Me.....	273
Configuring	275
Verifying Settings.....	276
Windows 2000/NT/XP	276
Verifying Settings.....	280
Macintosh OS 8/9.....	281
Verifying Settings.....	282
Macintosh OS X	282
Verifying Settings.....	284
Appendix D	
IP Subnetting	285
IP Addressing.....	285
IP Classes	285
Subnet Masks	286
Subnetting	286
Example: Two Subnets	287
Example: Four Subnets.....	289
Example Eight Subnets.....	290
Subnetting With Class A and Class B Networks.....	291
Appendix E	
Services	293
Appendix F	
Firewall Commands	297
Sys Firewall Commands	297
Appendix G	
Triangle Route	299

The Ideal Setup	299
The "Triangle Route" Problem	299
The "Triangle Route" Solutions	300
IP Aliasing	300
Gateways on the WAN Side	301
Appendix H	
Log Descriptions	303
Log Commands	312
Configuring What You Want the ZyXEL Device to Log	312
Displaying Logs	313
Log Command Example	314
Appendix I	
Command Interpreter	315
Command Syntax	315
Command Usage	315
Appendix J	
Internal SPTGEN	317
Internal SPTGEN Overview	317
The Configuration Text File Format	317
Internal SPTGEN File Modification - Important Points to Remember	317
Internal SPTGEN FTP Download Example	318
Internal SPTGEN FTP Upload Example	319
Command Examples	340
Index	343

List of Figures

Figure 1 Internet Access Application	40
Figure 2 Internet Telephony Service Provider Application	41
Figure 3 Peer-to-peer Calling	41
Figure 4 Firewall Application	42
Figure 5 LEDs	42
Figure 6 Password Screen	46
Figure 7 Change Password Screen	46
Figure 8 Wizard or Advanced Screen	47
Figure 9 Main Screen	48
Figure 10 Select a Mode	53
Figure 11 Wizard Welcome	54
Figure 12 Auto Detection: No DSL Connection	54
Figure 13 Auto-Detection: PPPoE	55
Figure 14 Auto Detection: Failed	55
Figure 15 Internet Access Wizard Setup: ISP Parameters	56
Figure 16 Internet Connection with PPPoE	57
Figure 17 Internet Connection with RFC 1483	58
Figure 18 Internet Connection with ENET ENCAP	58
Figure 19 Internet Connection with PPPoA	59
Figure 20 Connection Test Failed-2.	60
Figure 21 VoIP Phone Calls	61
Figure 22 Select a Mode	62
Figure 23 Wizard: Welcome	62
Figure 24 VoIP Wizard Configuration	63
Figure 25 SIP Registration Test	64
Figure 26 VoIP Wizard Fail	65
Figure 27 VoIP Wizard Finish	65
Figure 28 Select a Mode	69
Figure 29 Wizard: Welcome	69
Figure 30 Bandwidth Management Wizard: General Information	69
Figure 31 Bandwidth Management Wizard: Service Configuration	70
Figure 32 Bandwidth Management Wizard: Complete	71
Figure 33 Status Screen	73
Figure 34 Any IP Table	76
Figure 35 Packet Statistics	77
Figure 36 VoIP Statistics	79
Figure 37 Example of Traffic Shaping	85
Figure 38 Internet Access Setup (PPPoE)	87

Figure 39 Advanced Internet Access Setup	89
Figure 40 WAN More Connections	91
Figure 41 Traffic Redirect Example	92
Figure 42 Traffic Redirect LAN Setup	93
Figure 43 LAN and WAN IP Addresses	95
Figure 44 Any IP Example	100
Figure 45 LAN IP	101
Figure 46 Advanced LAN Setup	102
Figure 47 DHCP Setup	103
Figure 48 LAN Client List	105
Figure 49 Physical Network & Partitioned Logical Networks	106
Figure 50 LAN IP Alias	106
Figure 51 How NAT Works	110
Figure 52 NAT Application With IP Alias	111
Figure 53 NAT General	113
Figure 54 Multiple Servers Behind NAT Example	115
Figure 55 Port Forwarding	115
Figure 56 Port Forwarding Rule Setup	116
Figure 57 Network > NAT > ALG	118
Figure 58 SIP User Agent	121
Figure 59 SIP Proxy Server	122
Figure 60 SIP Redirect Server	123
Figure 61 SIP > SIP Settings	124
Figure 62 VoIP > SIP Settings > Advanced	128
Figure 63 DiffServ: Differentiated Service Field	132
Figure 64 SIP > QoS	132
Figure 65 Phone > Analog Phone	134
Figure 66 Phone > Analog Phone > Advanced	135
Figure 67 Phone > Common	137
Figure 68 VoIP > Phone > Region	141
Figure 69 Phone Book > Speed Dial	142
Figure 70 Phone Book > Incoming Call Policy	144
Figure 71 PSTN Line > General	146
Figure 72 Firewall Application	151
Figure 73 Three-Way Handshake	152
Figure 74 SYN Flood	153
Figure 75 Smurf Attack	154
Figure 76 Stateful Inspection	155
Figure 77 Firewall: General	164
Figure 78 Firewall Rules	166
Figure 79 Firewall: Edit Rule	168
Figure 80 Firewall: Customized Services	170
Figure 81 Firewall: Configure Customized Services	171

Figure 82 Firewall Example: Rules	172
Figure 83 Edit Custom Port Example	172
Figure 84 Firewall Example: Edit Rule: Destination Address	173
Figure 85 Firewall Example: Edit Rule: Select Customized Services	174
Figure 86 Firewall Example: Rules: MyService	175
Figure 87 Firewall: Threshold	177
Figure 88 Content Filter: Keyword	179
Figure 89 Content Filter: Schedule	180
Figure 90 Content Filter: Trusted	181
Figure 91 Example of Static Routing Topology	183
Figure 92 Static Route	184
Figure 93 Static Route Edit	185
Figure 94 Subnet-based Bandwidth Management Example	188
Figure 95 Bandwidth Management: Summary	191
Figure 96 Bandwidth Management: Rule Setup	193
Figure 97 Bandwidth Management Rule Configuration	194
Figure 98 Bandwidth Management: Monitor	196
Figure 99 Dynamic DNS	198
Figure 100 Remote Management: WWW	202
Figure 101 Telnet Configuration on a TCP/IP Network	203
Figure 102 Remote Management: Telnet	204
Figure 103 Remote Management: FTP	205
Figure 104 SNMP Management Model	206
Figure 105 Remote Management: SNMP	208
Figure 106 Remote Management: DNS	209
Figure 107 Remote Management: ICMP	210
Figure 108 Configuring UPnP	212
Figure 109 Add/Remove Programs: Windows Setup: Communication	214
Figure 110 Add/Remove Programs: Windows Setup: Communication: Components 214	
Figure 111 Network Connections	215
Figure 112 Windows Optional Networking Components Wizard	215
Figure 113 Networking Services	216
Figure 114 Network Connections	217
Figure 115 Internet Connection Properties	218
Figure 116 Internet Connection Properties: Advanced Settings	219
Figure 117 Internet Connection Properties: Advanced Settings: Add	219
Figure 118 System Tray Icon	220
Figure 119 Internet Connection Status	220
Figure 120 Network Connections	221
Figure 121 Network Connections: My Network Places	222
Figure 122 Network Connections: My Network Places: Properties: Example	222
Figure 123 System General Setup	224

Figure 124 System Time Setting	225
Figure 125 View Log	230
Figure 126 Log Settings	231
Figure 127 E-mail Log Example	234
Figure 128 Firmware Upgrade	237
Figure 129 Firmware Upload In Progress	237
Figure 130 Network Temporarily Disconnected	238
Figure 131 Error Message	238
Figure 132 Configuration	239
Figure 133 Configuration Upload Successful	240
Figure 134 Network Temporarily Disconnected	240
Figure 135 Reset Warning Message	240
Figure 136 Reset In Process Message	241
Figure 137 Restart Screen	241
Figure 138 FTP Session Example	242
Figure 139 Restore Using FTP Session Example	245
Figure 140 FTP Session Example of Firmware File Upload	246
Figure 141 Diagnostic: General	249
Figure 142 Diagnostic: DSL Line	250
Figure 143 Pop-up Blocker	256
Figure 144 Internet Options	257
Figure 145 Internet Options	258
Figure 146 Pop-up Blocker Settings	259
Figure 147 Internet Options	260
Figure 148 Security Settings - Java Scripting	261
Figure 149 Security Settings - Java	262
Figure 150 Java (Sun)	263
Figure 151 Outgoing Calls: Both Phone Ports - SIP1	264
Figure 152 Outgoing Calls: Individual SIP Accounts	265
Figure 153 Incoming Calls: Both SIP Accounts	265
Figure 154 Incoming Calls: Individual SIP Accounts	266
Figure 155 Connecting a POTS Splitter	271
Figure 156 Connecting a Microfilter	272
Figure 157 Windows 95/98/Me: Network: Configuration	274
Figure 158 Windows 95/98/Me: TCP/IP Properties: IP Address	275
Figure 159 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	276
Figure 160 Windows XP: Start Menu	277
Figure 161 Windows XP: Control Panel	277
Figure 162 Windows XP: Control Panel: Network Connections: Properties	278
Figure 163 Windows XP: Local Area Connection Properties	278
Figure 164 Windows XP: Advanced TCP/IP Settings	279
Figure 165 Windows XP: Internet Protocol (TCP/IP) Properties	280
Figure 166 Macintosh OS 8/9: Apple Menu	281

Figure 167 Macintosh OS 8/9: TCP/IP	282
Figure 168 Macintosh OS X: Apple Menu	283
Figure 169 Macintosh OS X: Network	283
Figure 170 Ideal Setup	299
Figure 171 "Triangle Route" Problem	300
Figure 172 IP Alias	300
Figure 173 Gateways on the WAN Side	301
Figure 174 Displaying Log Categories Example	312
Figure 175 Displaying Log Parameters Example	313
Figure 176 Log Command Example	314
Figure 177 Configuration Text File Format: Column Descriptions	317
Figure 178 Invalid Parameter Entered: Command Line Example	318
Figure 179 Valid Parameter Entered: Command Line Example	318
Figure 180 Internal SPTGEN FTP Download Example	319
Figure 181 Internal SPTGEN FTP Upload Example	319

List of Tables

Table 1 Models Covered	35
Table 2 ADSL Standards	36
Table 3 LEDs	43
Table 4 Web Configurator Icons in the Title Bar	49
Table 5 Navigation Panel Summary	49
Table 6 Internet Access Wizard Setup: ISP Parameters	56
Table 7 Internet Connection with PPPoE	57
Table 8 Internet Connection with RFC 1483	58
Table 9 Internet Connection with ENET ENCAP	59
Table 10 Internet Connection with PPPoA	59
Table 11 Sample SIP Account Information	63
Table 12 VoIP Wizard Configuration	63
Table 13 Media Bandwidth Management Setup: Services	67
Table 14 Bandwidth Management Wizard: General Information	70
Table 15 Bandwidth Management Wizard: Service Configuration	70
Table 16 Status Screen	74
Table 17 Any IP Table	76
Table 18 Packet Statistics	77
Table 19 VoIP Statistics	79
Table 20 Internet Access Setup	87
Table 21 Advanced Internet Access Setup	89
Table 22 Advanced Internet Access Setup	91
Table 23 WAN Backup Setup	94
Table 24 LAN IP	101
Table 25 Advanced LAN Setup	102
Table 26 DHCP Setup	103
Table 27 LAN Client List	105
Table 28 LAN IP Alias	107
Table 29 NAT Definitions	109
Table 30 NAT Mapping Types	112
Table 31 NAT General	113
Table 32 Services and Port Numbers	114
Table 33 Port Forwarding	116
Table 34 Port Forwarding Rule Setup	117
Table 35 Network > NAT > ALG	118
Table 36 SIP Call Progression	120
Table 37 SIP > SIP Settings	124
Table 38 Custom Tones Details	126

Table 39 VoIP > SIP Settings > Advanced	129
Table 40 SIP > QoS	132
Table 41 Phone > Analog Phone	134
Table 42 Phone > Analog Phone > Advanced	135
Table 43 Phone > Common	137
Table 44 European Flash Key Commands	138
Table 45 USA Flash Key Commands	140
Table 46 VoIP > Phone > Region	141
Table 47 Phone Book > Speed Dial	142
Table 48 Phone Book > Incoming Call Policy	144
Table 49 PSTN Line > General	146
Table 50 Common IP Ports	152
Table 51 ICMP Commands That Trigger Alerts	154
Table 52 Legal NetBIOS Commands	154
Table 53 Legal SMTP Commands	154
Table 54 Firewall: General	165
Table 55 Firewall Rules	166
Table 56 Firewall: Edit Rule	169
Table 57 Customized Services	170
Table 58 Firewall: Configure Customized Services	171
Table 59 Firewall: Threshold	177
Table 60 Content Filter: Keyword	180
Table 61 Content Filter: Schedule	181
Table 62 Content Filter: Trusted	181
Table 63 Static Route	184
Table 64 Static Route Edit	185
Table 65 Application and Subnet-based Bandwidth Management Example	188
Table 66 Maximize Bandwidth Usage Example	189
Table 67 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example 190	
Table 68 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example 190	
Table 69 Bandwidth Management Priorities	191
Table 70 Media Bandwidth Management: Summary	192
Table 71 Bandwidth Management: Rule Setup	193
Table 72 Bandwidth Management Rule Configuration	194
Table 73 Dynamic DNS	198
Table 74 Remote Management: WWW	203
Table 75 Remote Management: Telnet	204
Table 76 Remote Management: FTP	205
Table 77 SNMP Traps	207
Table 78 Remote Management: SNMP	208
Table 79 Remote Management: DNS	209

Table 80 Remote Management: ICMP	210
Table 81 Configuring UPnP	213
Table 82 System General Setup	224
Table 83 System Time Setting	225
Table 84 View Log	230
Table 85 Log Settings	231
Table 86 SMTP Error Messages	233
Table 87 Filename Conventions	236
Table 88 Firmware Upgrade	237
Table 89 Restore Configuration	239
Table 90 General Commands for GUI-based FTP Clients	242
Table 91 General Commands for GUI-based TFTP Clients	244
Table 92 Diagnostic: General	249
Table 93 Diagnostic: DSL Line	250
Table 94 Troubleshooting Starting Up Your Device	253
Table 95 Troubleshooting the LAN	253
Table 96 Troubleshooting the WAN	254
Table 97 Troubleshooting Accessing Your Device	255
Table 98 Troubleshooting Telephone	263
Table 99 Device Specifications	267
Table 100 Firmware Specifications	268
Table 101 ZyXEL Device Power Adaptor Specifications	269
Table 102 Classes of IP Addresses	285
Table 103 Allowed IP Address Range By Class	286
Table 104 "Natural" Masks	286
Table 105 Alternative Subnet Mask Notation	287
Table 106 Two Subnets Example	287
Table 107 Subnet 1	288
Table 108 Subnet 2	288
Table 109 Subnet 1	289
Table 110 Subnet 2	289
Table 111 Subnet 3	289
Table 112 Subnet 4	290
Table 113 Eight Subnets	290
Table 114 Class C Subnet Planning	290
Table 115 Class B Subnet Planning	291
Table 116 Examples of Services	293
Table 117 Sys Firewall Commands	297
Table 118 System Maintenance Logs	303
Table 119 System Error Logs	304
Table 120 Access Control Logs	304
Table 121 TCP Reset Logs	305
Table 122 Packet Filter Logs	305

Table 123 ICMP Logs	305
Table 124 CDR Logs	306
Table 125 PPP Logs	306
Table 126 UPnP Logs	307
Table 127 Content Filtering Logs	307
Table 128 Attack Logs	307
Table 129 802.1X Logs	308
Table 130 ACL Setting Notes	309
Table 131 ICMP Notes	309
Table 132 Syslog Logs	310
Table 133 SIP Logs	310
Table 134 RTP Logs	311
Table 135 FSM Logs: Caller Side	311
Table 136 FSM Logs: Callee Side	311
Table 137 Lifeline Logs	311
Table 138 RFC-2408 ISAKMP Payload Types	312
Table 139 Abbreviations Used in the Example Internal SPTGEN Screens Table ..	319
Table 140 Menu 1 General Setup	320
Table 141 Menu 3	320
Table 142 Menu 4 Internet Access Setup	323
Table 143 Menu 12	325
Table 144 Menu 15 SUA Server Setup	329
Table 145 Menu 21.1 Filter Set #1	331
Table 146 Menu 21.1 Filter Set #2,	334
Table 147 Menu 23 System Menus	339
Table 148 Menu 24.11 Remote Management Control	340
Table 149 Command Examples	340

Preface

Congratulations on your purchase of the P-2602R/RL-DxA ADSL2+ VoIP IAD.

Your ZyXEL Device is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your ZyXEL Device for its various applications.

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

Related Documentation

- Supporting Disk

Refer to the included CD for support documents.

- Quick Start Guide

The Quick Start Guide is designed to help you get up and running right away. It contains 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

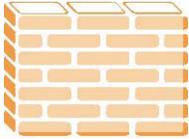
Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choices.
- Screen titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- 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-2602R/RL-DxA may be referred to as the ZyXEL Device in this user's guide.

Graphics Icons Key

ZyXEL Device 	Computer 	Notebook computer 
Server 	Switch 	Router 
Telephone 	DSLAM 	Trunking gateway 
Firewall 	Wireless signal 	

CHAPTER 1

Getting To Know the ZyXEL Device

This chapter describes the key features and applications of your device.

1.1 Introducing the P-2602RL-DxA Series

The P-2602R/RL-DxA series are Integrated Access Devices (IADs) that combine an ADSL2+ router with Voice over IP (VoIP) communication capabilities to allow you to use a traditional analog telephone to make Internet calls. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The P-2602R/RL-DxA series is also a complete security solution with a robust firewall and content filtering.

At the time of writing, this guide covers the following models.

Table 1 Models Covered

P-2602R-D1A	P-2602R-D3A	P-2602R-D7A
P-2602RL-D1A	P-2602RL-D3A	P-2602RL-D7A

Not all models include all features. Please refer to the following description of the product name format.

- “R” denotes an integrated router. The “R” models also include Virtual Private Network (VPN) capability.
- “L” denotes the PSTN (Public Switched Telephone Network) line feature. The PSTN line lets you have VoIP phone service and PSTN phone service at the same time.

Note: When the ZyXEL Device does not have power, only the phone connected to the **PHONE 2** port can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.

Models with “3” as the next to the last character (like the P-2602RL-D3A) denote a device that works over ISDN (Integrated Services Digital Network). Models with “1” or “7” as the next to the last character (like the P-2602RL-D1A or the P-2602RL-D7A) denote a device that works over T-ISDN (UR-2).

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

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

1.2 Features

The following sections introduce your device's key features.

Ethernet Port

The 10/100 Mbps auto-negotiating Ethernet port allows the device to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. The port is auto-crossover (MDI/MDI-X) meaning it automatically adjusts to either a crossover or straight-through Ethernet cable.

High Speed Internet Access

The ZyXEL Device is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks. The ZyXEL Device is an ADSL router compatible with the ADSL/ADSL2/ADSL2+ standards. Maximum data rates attainable by the ZyXEL Device for each standard are shown in the next table.

Table 2 ADSL Standards

STANDARD	UPSTREAM DATA RATE	DOWNSTREAM DATA RATE
ADSL	832 kbps	8 Mbps
ADSL2	1 Mbps	12 Mbps
ADSL2+	1 Mbps	24 Mbps

Note: The standard your ISP uses determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, line quality, your subscribed level of service and other factors.

PSTN Line (“L” Models only)

You can connect a PSTN line to your device. You can receive incoming PSTN phone calls even while someone else is making VoIP phone calls. You can dial a (prefix) number to make an outgoing PSTN call. You can still make PSTN phone calls if your device loses power.

Note: When the ZyXEL Device does not have power, only the phone connected to the **PHONE 2** port can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.

Zero Configuration Internet Access

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

Auto Provisioning

Your VoIP service provider can automatically update your device's configuration via an auto-provisioning server.

Auto Firmware Upgrade

Your device gives you the option to upgrade to a newer firmware version if it finds one during auto-provisioning. Your VoIP service provider must have an auto-provisioning server and a server set up with firmware in order for this feature to work.

Firewall

Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

Content Filtering

Content filtering allows you to block access to Internet web sites that contain key words (that you specify) in the URL. You can also schedule when to perform the filtering and give trusted LAN IP addresses unfiltered Internet access.

Media Bandwidth Management

Media Bandwidth Management allows you to specify bandwidth classes based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth classes.

Dynamic Jitter Buffer

The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.

Multiple SIP Accounts

You can simultaneously use multiple voice (SIP) accounts and assign them to one or both telephone ports.

Multiple Voice Channels

Your device can simultaneously handle multiple voice channels (telephone calls). Additionally you can answer an incoming phone call on a VoIP account, even while someone else is using the account for a phone call.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.

Comfort Noise Generation

Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).

Echo Cancellation

Your device supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

QoS (Quality of Service)

Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network.

SIP ALG

Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).

Universal Plug and Play (UPnP)

Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other.

PPPoE Support (RFC2516)

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

Other PPPoE Features

- PPPoE idle time out
- PPPoE dial on demand

Dynamic DNS Support

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

DHCP

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

Multiple PVC (Permanent Virtual Circuits) Support

Your device supports up to 8 Permanent Virtual Circuits (PVC's).

IP Alias

IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.

IP Policy Routing (IPPR)

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

Packet Filters

Your device's packet filtering function allows added network security and management.

Ease of Installation

Your device is designed for quick, intuitive and easy installation.

Housing

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

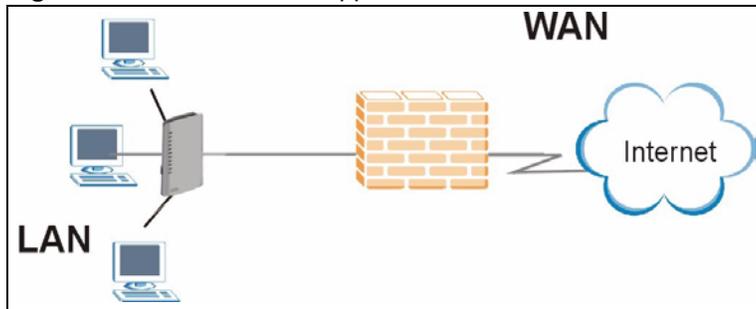
1.3 Applications for the ZyXEL Device

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

1.3.1 Internet Access

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

Figure 1 Internet Access Application



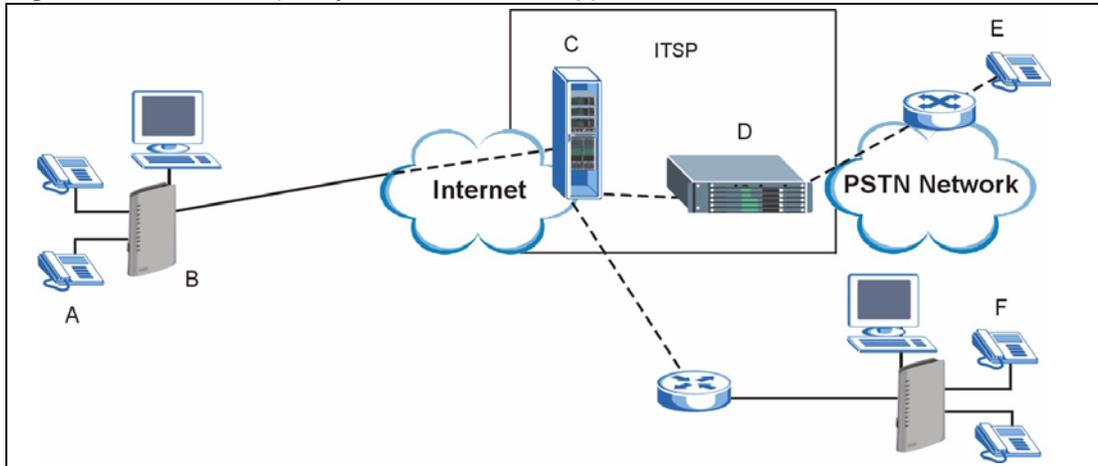
1.3.1.1 Internet Single User Account

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

1.3.2 Making Calls via Internet Telephony Service Provider

In a home or small office environment, you can use your device to make and receive VoIP telephone calls through an Internet Telephony Service Provider (ITSP).

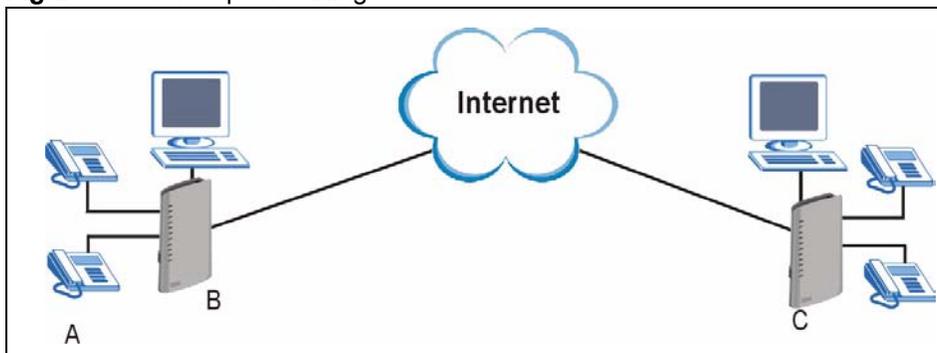
The following figure shows a basic example of how you would make a VoIP call through an ITSP. You use your analog phone (A in the figure) and your device (B) changes the call into VoIP. Your device then sends your call to the Internet and the ITSP's SIP server. The VoIP call server forwards calls to PSTN phones (E) through a trunking gateway (D) to the PSTN network. The VoIP call server forwards calls to IP phones (F) through the Internet.

Figure 2 Internet Telephony Service Provider Application

1.3.3 Make Peer-to-peer Calls

You can call directly to someone's IP address without using a SIP proxy server. Peer-to-peer calls are also called "Point to Point" or "IP-to-IP" calls. You must know the peer's IP address in order to do this.

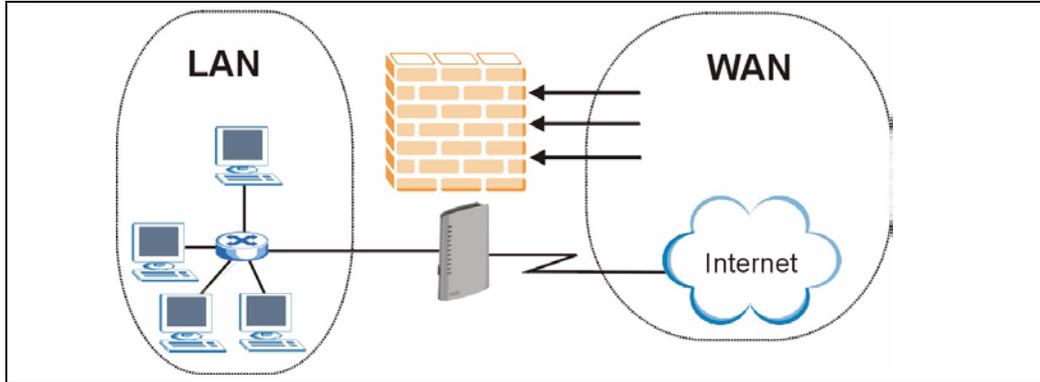
The following figure shows a basic example of how you would make a peer-to-peer VoIP call. You use your analog phone (A in the figure) and your device (B) changes the call into VoIP, and sends the call through the Internet to the peer VoIP device (C).

Figure 3 Peer-to-peer Calling

1.3.4 Firewall for Secure Broadband Internet Access

Your device provides protection from attacks by Internet hackers. By default, the firewall blocks all incoming traffic from the WAN. The firewall supports TCP/UDP inspection and DoS (Denial of Services) detection and prevention, as well as real time alerts, reports and logs.

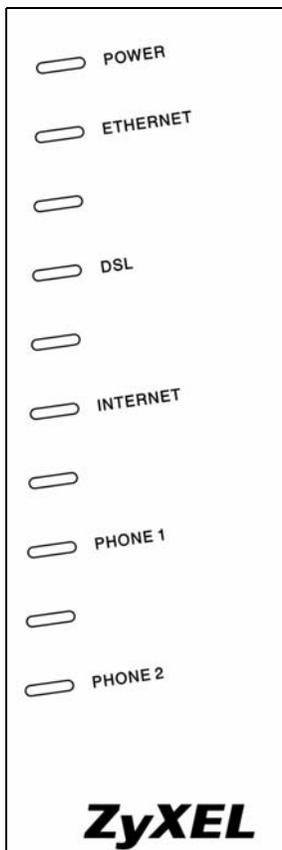
Figure 4 Firewall Application



1.3.5 LEDs

The LED display can help you determine the status of your ZyXEL Device. Look on either side of your ZyXEL Device to see the LEDs.

Figure 5 LEDs



The following table describes your device's LEDs.

Table 3 LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	Your device is receiving power and functioning properly.
		Blinking	Your device is rebooting and performing a self-test.
	Red	On	Your device is not receiving enough power.
	None	Off	Your device is not ready or has malfunctioned.
ETHERNET	Green	On	Your device has a successful Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
	None	Off	The LAN is not connected.
DSL	Green	On	Your device has a physical connection with the ISP.
		Blinking	Your device is initializing the DSL line.
	None	Off	The DSL link is down.
INTERNET	Green	On	Your device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	Your device is sending or receiving IP traffic.
	Red	On	Your device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed).
	None	Off	Your device does not have an IP connection
PHONE 1, 2	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is voice message in the corresponding SIP account.
	None	Off	The phone port does not have a SIP account registered.

Refer to the Quick Start Guide for information on hardware connections.

CHAPTER 2

Introducing the Web Configurator

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

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy 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).

See [Chapter 24 on page 253](#) if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

- 1** Make sure your ZyXEL Device hardware is properly connected (refer to the *Quick Start Guide*).
- 2** Launch your web browser.
- 3** Type "192.168.1.1" as the URL.
- 4** A password screen displays. The default password ("1234") displays in non-readable characters. If you haven't changed the password yet, you can just click **Login**. Click **Cancel** to revert to the default password in the password field. If you have changed the password, enter your password and click **Login**.

Figure 6 Password ScreenThe image shows the password login screen for a ZyXEL P-2602RL-D1A router. At the top, the ZyXEL logo is displayed in white on a blue background. Below the logo, the model number "P-2602RL-D1A" is centered. The text "Welcome to your router Configuration Interface" is followed by the instruction "Enter your password and press enter or click 'Login'". A password input field is shown with a key icon and the text "Password: ****". Below the input field are two buttons: "Login" and "Cancel".

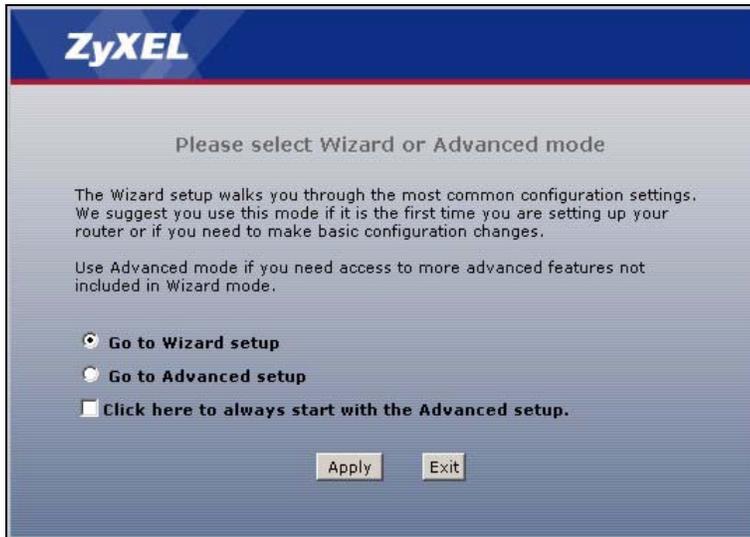
- 5 The following screen displays if you have not yet changed your password. It is highly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

Figure 7 Change Password ScreenThe image shows the change password screen for a ZyXEL router. At the top, the ZyXEL logo is displayed in white on a blue background. Below the logo, the text "Use this screen to change the password." is centered. The main text reads: "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." Below this text, it says "Enter your new password in the two fields below and click 'Apply'. Otherwise click 'Ignore' to keep the default password". There are two input fields: "New Password:" and "Retype to Confirm:". Below the input fields are two buttons: "Apply" and "Ignore".

- 6 A screen displays to let you choose whether to go to the wizard or the advanced screens.
- Click **Go to Wizard setup** if you are logging in for the first time or if you want to make basic changes. The wizard selection screen appears after you click **Apply**. See [Chapter 3 on page 53](#) for more information.
 - Click **Go to Advanced setup** if you want to configure features that are not available in the wizards. Select the check box if you always want to go directly to the advanced screens. The main screen appears after you click **Apply**. See [Section 2.2 on page 48](#) for more information.
 - Click **Exit** if you want to log out.

Note: For security reasons, the ZyXEL Device automatically logs you out if you do not use the web configurator for five minutes. If this happens, log in again.

Figure 8 Wizard or Advanced Screen



2.1.2 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button 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”.

2.1.2.1 Using The Reset Button

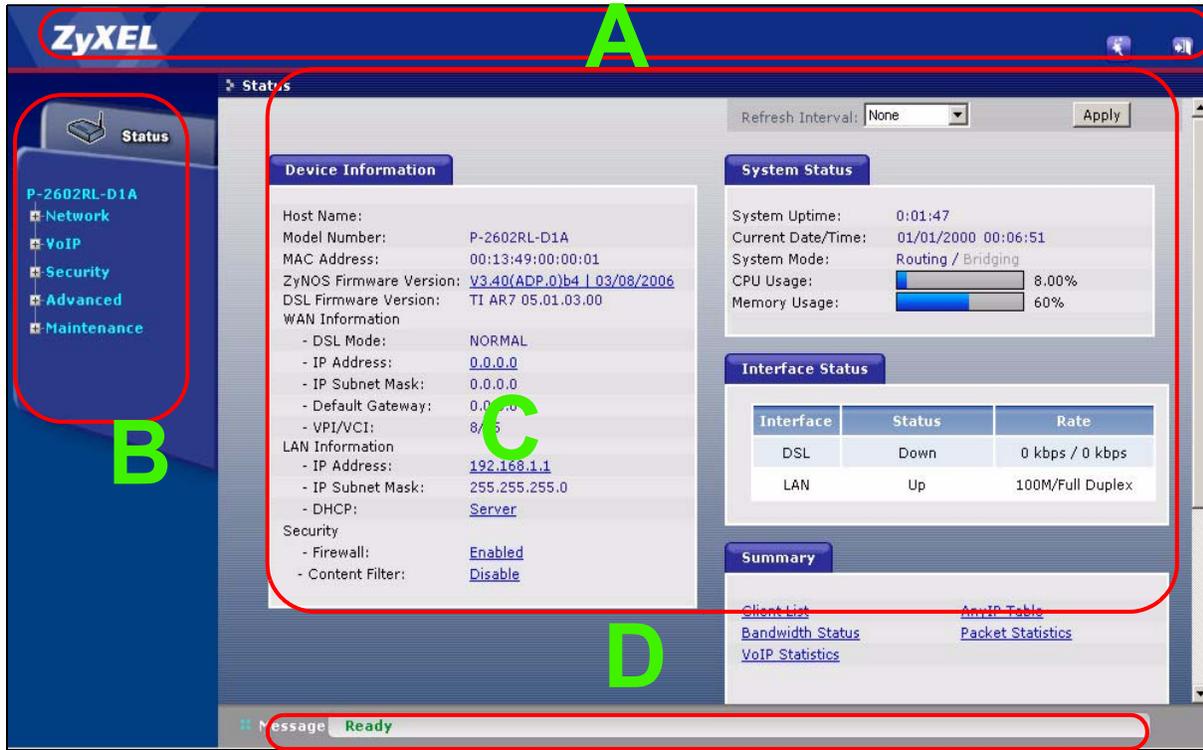
- 1 Make sure the **POWER LED** is on (not blinking).
- 2 Do one of the following.

To restart the device, press the **RESET** button for one second and release it.

To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER LED** begins to blink and then release it. When the **POWER LED** begins to blink, the defaults have been restored and the device restarts.

2.2 Web Configurator Main Screen

Figure 9 Main Screen



As illustrated above, the main screen is divided into these parts:

- A - title bar
- B - navigation panel
- C - main window
- D - status bar

2.2.1 Title Bar

The title bar allows you to change the language and provides some icons in the upper right corner.



The icons provide the following functions.

Table 4 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Wizards: Click this icon to go to the configuration wizards. See Chapter 3 on page 53 for more information.
	Logout: Click this icon to log out of the web configurator.

2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following tables describe each menu item.

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen contains administrative and system-related information.
Network		
WAN	Internet Access Setup	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to configure additional Internet access connections.
	WAN Backup Setup	Use this screen to configure a backup gateway for your WAN.
LAN	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names).
	IP Alias	Use this screen to partition your LAN interface into subnets.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	ALG	Use this screen to enable and disable the SIP (VoIP) ALG in the ZyXEL Device.
VoIP		
SIP	SIP Settings	Use this screen to configure your ZyXEL Device's Voice over IP settings.
	QoS	Use this screen to configure your ZyXEL Device's Quality of Service settings for VoIP.
Phone	Analog Phone	Use this screen to set which phone ports use which SIP accounts.
	Common	Use this screen to configure general phone port settings.
	Region	Use this screen to select your location and call service mode.

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
Phone Book	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
	Incoming Call Policy	Use this screen to configure call-forwarding.
PSTN Line	General	Use this screen to configure your ZyXEL Device's settings for PSTN calls.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
	Threshold	Use this screen to configure the thresholds for determining when to drop sessions that do not become fully established.
Content Filter	Keyword	Use this screen to block access to web sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for your device to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering.
Advanced		
Static Route	Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Bandwidth MGMT	Summary	Use this screen to configure bandwidth management on an interface.
	Rule Setup	Use this screen to define a bandwidth rule.
	Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
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.
	SNMP	Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
	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.
	ICMP	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
UPnP	General	Use this screen to turn UPnP on or off.
Maintenance		

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
	DSL Line	These screen displays information to help you identify problems with the DSL connection.

2.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See [Chapter 6 on page 73](#) for more information about the **Status** screen.

2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

CHAPTER 3

Internet Setup Wizard

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

3.1 Introduction

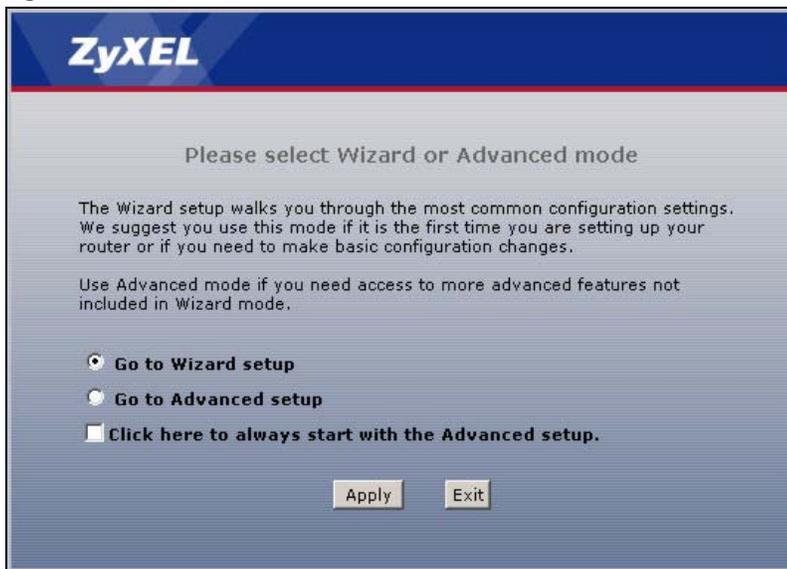
Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.

Note: See the advanced menu chapters for background information on these fields.

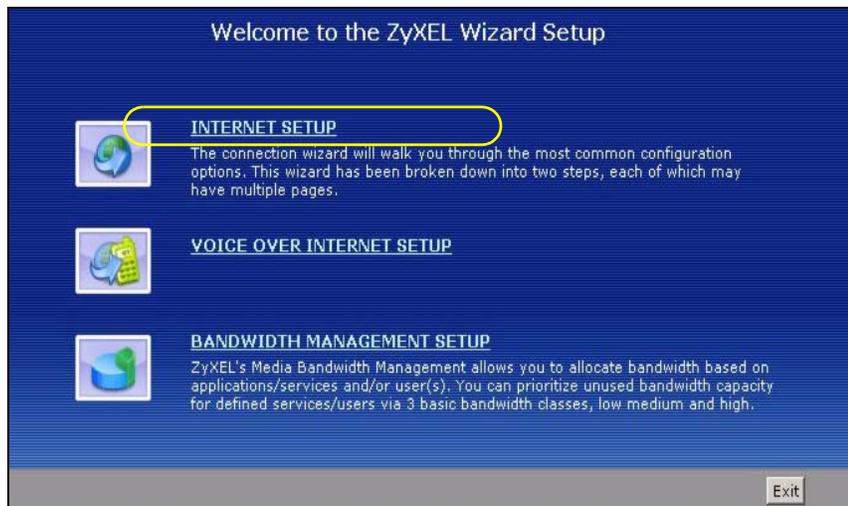
3.2 Internet Access Wizard Setup

- 1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon () in the top right corner of the web configurator to go to the wizards.

Figure 10 Select a Mode



- 2 Click **INTERNET/WIRELESS SETUP** to configure the system for Internet access and wireless connection.

Figure 11 Wizard Welcome

- 3 Your ZyXEL device attempts to detect your DSL connection and your connection type.
 - a The following screen appears if a connection is not detected. Check your hardware connections and click **Restart the Internet/Wireless Setup Wizard** to return to the wizard welcome screen.

Figure 12 Auto Detection: No DSL Connection

- b The following screen displays if a PPPoE or PPPoA connection is detected. Enter your Internet account information (username, password and/or service name) exactly as provided by your ISP.

Figure 13 Auto-Detection: PPPoE

The screenshot shows a web-based configuration wizard titled "Internet Configuration" with a progress bar indicating "STEP 1" and "STEP 2". Under the "Auto-Detected ISP" section, the "Connection Type" is set to "PPP over Ethernet (PPPoE)". Below this, the "ISP Parameters for Internet Access" section contains a message: "Please enter the User Name and Password given to you by your Internet Service Provider here. If your ISP gave you a Service Name, enter it in the third field". There are three input fields: "User Name", "Password", and "Service Name" (with "(optional)" to its right). At the bottom, there are three buttons: "< Back", "Next >", and "Exit".

- c The following screen appears if the ZyXEL device detects a connection but not the connection type. Click **Next** and refer to [Section 3.2.1 on page 55](#) on how to manually configure the ZyXEL Device for Internet access.

Figure 14 Auto Detection: Failed

The screenshot shows the same "Internet Configuration" wizard. The "Connection Type" field now displays the message: "Detection Failed. Please make sure the DSL cable is connected. Click the 'Next' button below to manually configure your Internet connection". Below this, there is a "Note" section with a yellow warning icon: "This wizard can only automatically detect PPP over Ethernet (PPPoE), PPP over ATM (PPPoA), or dynamically assigned Ethernet Internet connections. Your Internet connection may use a Static IP address which cannot be detected automatically." At the bottom, the "< Back", "Next >", and "Exit" buttons are visible.

3.2.1 Manual Configuration

- 1 If the ZyXEL Device fails to detect your DSL connection type but the physical line is connected, enter your Internet access information in the wizard screen exactly as your SIP gave it to you. Leave the defaults in any fields for which you were not given information.

Figure 15 Internet Access Wizard Setup: ISP Parameters

STEP 1 → **STEP 2**

Internet Configuration

ISP Parameters for Internet Access

Please verify the following settings with your Internet Service Provider (ISP). Your ISP may have given you a welcome letter or network setup letter including this information.

Mode
 Select 'Routing' (default) if your ISP allows multiple computers to share an Internet account. Otherwise, select 'Bridge' mode.

Encapsulation
 Select the encapsulation method used by your ISP. Your ISP may list 'ENET ENCAP' as 'Static IP' or 'Dynamic IP'.

Multiplexing
 Select the multiplexing type used by your ISP.

Virtual Circuit ID

VPI
VCI

Select the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) used by your ISP. The valid range for the VPI is 0 to 255 and VCI is 32 to 65535.

< Back Next > Exit

The following table describes the fields in this screen.

Table 6 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Mode	From the Mode drop-down list box, select Routing (default) if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box. Choices vary depending on what you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
Multiplexing	Select the multiplexing method used by your ISP from the Multiplex drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Back	Click Back to go back to the previous screen.
Next	Click Next to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.
Exit	Click Exit to close the wizard screen without saving your changes.

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

Figure 16 Internet Connection with PPPoE

STEP 1 | **STEP 2**

Internet Configuration

ISP Parameters for Internet Access
Please enter the User Name and Password given to you by your Internet Service Provider here. If your ISP gave you a Service Name, enter it in the third field

User Name

Password

Service Name (optional)

Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assign you a different one each time you connect to the Internet.

< Back Apply Exit

The following table describes the fields in this screen.

Table 7 Internet Connection with PPPoE

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Service Name	Type the name of your PPPoE service here.
Back	Click Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Exit	Click Exit to close the wizard screen without saving your changes.

Figure 17 Internet Connection with RFC 1483



The following table describes the fields in this screen.

Table 8 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select Routing in the Mode field. Type your ISP assigned IP address in this field.
Back	Click Back to go back to the previous wizard screen.
Next	Click Next to continue to the next wizard screen.
Exit	Click Exit to close the wizard screen without saving your changes.

Figure 18 Internet Connection with ENET ENCAP



The following table describes the fields in this screen.

Table 9 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select Obtain an IP Address Automatically if you have a dynamic IP address.
Static IP Address	Select Static IP Address if your ISP gave you an IP address to use.
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask If you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use ENET ENCAP in the Encapsulation field in the previous screen.
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Exit	Click Exit to close the wizard screen without saving your changes.

Figure 19 Internet Connection with PPPoA

The screenshot shows a blue-themed wizard screen. At the top, it says 'STEP 1' and 'Internet Configuration'. Below that, it says 'ISP Parameters for Internet Access' and 'Please enter the User Name and Password given to you by your Internet Service Provider here'. There are two input fields: 'User Name' and 'Password'. A yellow note icon is followed by the text: 'Note: Device is automatically configured to obtain an IP address automatically. The ISP will assign you a different one each time you connect to the Internet.' At the bottom right, there are three buttons: '< Back', 'Apply', and 'Exit'.

The following table describes the fields in this screen.

Table 10 Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.

Table 10 Internet Connection with PPPoA (continued)

LABEL	DESCRIPTION
Back	Click Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Exit	Click Exit to close the wizard screen without saving your changes.

- If the user name and/or password you entered for PPPoE or PPPoA connection are not correct, the screen displays as shown next. Click **Back to Username and Password setup** to go back to the screen where you can modify them.
- If the following screen displays, check if your account is activated or click **Restart the Internet/Wireless Setup Wizard** to verify your Internet access settings.

Figure 20 Connection Test Failed-2.

CHAPTER 4

VoIP Wizard And Example

This chapter shows you how to configure your SIP account(s) and make a VoIP phone call.

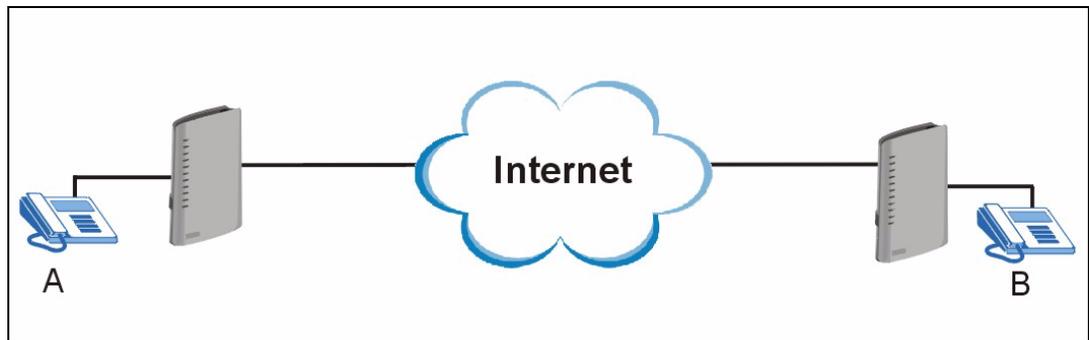
4.1 Introduction

The ZyXEL Device has Voice over IP (VoIP) communication capabilities that allow you to use a traditional analog telephone to make Internet calls. You can configure the ZyXEL Device to use up to two SIP based VoIP accounts.

This section describes how you can set up your ZyXEL Device to call someone who is also using a VoIP device. Make sure your telephone is connected to the **Phone 1** port before you start with our example.

In the following figure, **A** represents your phone and **B** represents the phone of the person you would like to call.

Figure 21 VoIP Phone Calls

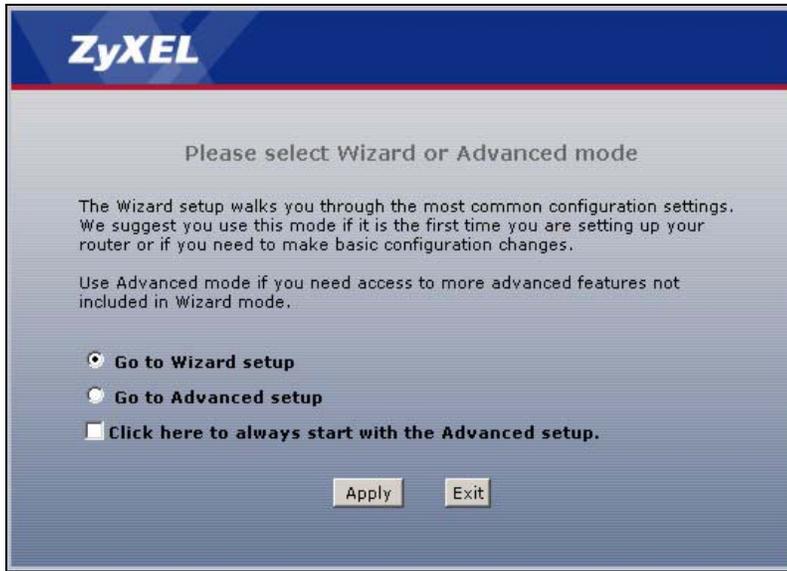


In order to make VoIP calls you need to register at least one SIP account on your ZyXEL Device. You can register your SIP account in the **VOICE OVER INTERNET SETUP** wizard.

4.2 VoIP Wizard Setup

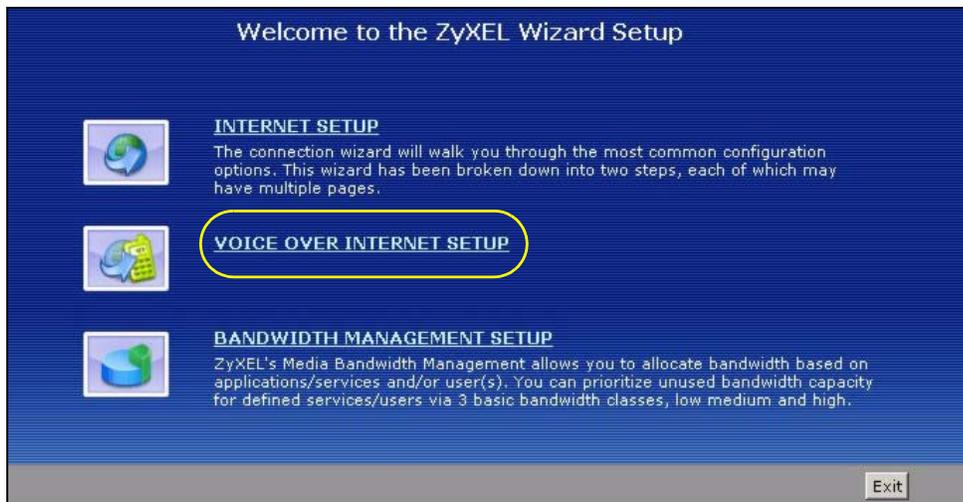
- 1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon () in the top right corner of the web configurator to display the wizard main screen.

Figure 22 Select a Mode



2 Click **VOICE OVER INTERNET SETUP** to configure your SIP settings.

Figure 23 Wizard: Welcome



- 3 Fill in the **VOICE OVER INTERNET SETUP** wizard screen with the information provided by your VoIP service provider. Your VoIP service provider supplies you with the following information. When you are finished, click **Apply**.

Table 11 Sample SIP Account Information

INFORMATION FROM VOIP SERVICE PROVIDER	EXAMPLE VALUES	DESCRIPTION
SIP account address	11223344@SIPA-Account.com	11223344 is your SIP number. This is the part that comes before the “@” symbol in your SIP account address. SIPA-Account.com is your SIP server domain.
SIP server address	a.b.c.d	a.b.c.d is the IP address or domain name of your SIP server.
Username	VoIPUser	This is the username you use to login to your SIP account.
Password	Password	This is the password you use to login to your SIP account.

Figure 24 VoIP Wizard Configuration

The following table describes the labels in this screen.

Table 12 VoIP Wizard Configuration

LABEL	DESCRIPTION
SIP Number	Enter your SIP number in this field. Use the number or text that comes before the @ symbol in a SIP account. If your SIP account is 11223344@SIPA-Account.com , your SIP number is “11223344”. You can use up to 127 ASCII characters.
SIP Server Address	Type the IP address or domain name of the SIP server in this field. It doesn't matter whether the SIP server is a proxy, redirect or register server. You can use up to 95 ASCII characters.

Table 12 VoIP Wizard Configuration

LABEL	DESCRIPTION
SIP Service Domain	Enter the SIP service domain name in this field (the domain name that comes after the @ symbol in a SIP account like 11223344@SIP-Account.com). You can use up to 127 ASCII Extended set characters.
User Name	This is the name used to register this SIP account with the SIP register server. Type the user name exactly as it was given to you. You can use up to 95 ASCII characters.
Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Check here to set up SIP2 settings.	This screen configures SIP account 1. Select the check box if you have a second SIP account that you want to use. You will need to configure the same fields for the second SIP account. Note: If you configure more than one SIP account, you need to configure Analog Phone settings in Section 10.12 on page 134 to distinguish between the two accounts when you make and receive phone calls.
Back	Click Back to return to the previous screen.
Apply	Click Apply to complete the wizard setup and save your configuration.
Exit	Click Exit to close the wizard without saving your settings.

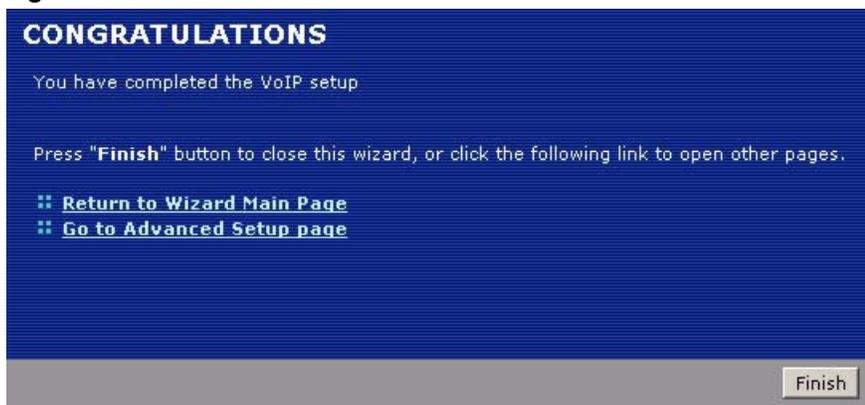
- 4 Your ZyXEL Device will attempt to register your SIP account with your VoIP service provider. When your account is registered your **PHONE 1** light will come on and you are ready to make and receive VoIP phone calls.

Figure 25 SIP Registration Test

- 5 This screen displays if SIP account registration fails. If your DSL cable was disconnected, you can try connecting it. Then wait a few seconds and click **Register Again**. If your Internet connection was already working, you can click **Back** and try re-entering your SIP account settings.

Figure 26 VoIP Wizard Fail

- 6** This screen displays if your SIP account registration was successful. Click **Return to Wizard Main Page** if you want to use another configuration wizard. Click **Go to Advanced Setup page** or **Finish** to close the wizard and go to the main web configurator screens.

Figure 27 VoIP Wizard Finish

- 7** To call other VoIP users, you need to follow a similar process to ensure that their SIP account is registered and active. After it is registered, they need to provide you with their SIP number. You can use your VoIP service provider's dialing plan to call SIP numbers.
- You can also use your VoIP service provider's dialing plan to call regular phone numbers. You dial a prefix number, provided to you by your VoIP service provider, followed by a regular phone number.

Note: To find out more information about configuring your VoIP features and making non VoIP calls see [Chapter 10 on page 119](#).

CHAPTER 5

Bandwidth Management Wizard

This chapter shows you how to configure basic bandwidth management using the wizard screens.

5.1 Introduction

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

5.2 Predefined Media 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 13 Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
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.
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses TCP (Transmission Control Protocol) 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
Telnet	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. Telnet uses TCP port 23.

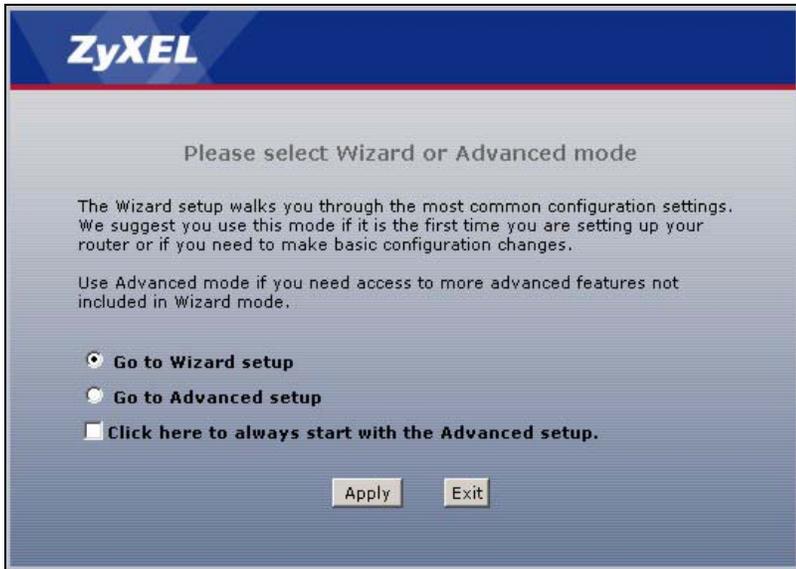
Table 13 Media Bandwidth Management Setup: Services (continued)

SERVICE	DESCRIPTION
NetMeeting (H.323)	<p>A multimedia communications product from Microsoft that enables groups to teleconference and videoconference over the Internet. NetMeeting supports VoIP, text chat sessions, a whiteboard, and file transfers and application sharing.</p> <p>NetMeeting uses H.323. H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service.</p> <p>H.323 is transported primarily over TCP, using the default port number 1720.</p>
VoIP (SIP)	<p>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.</p> <p>SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.</p>
VoIP (H.323)	<p>Sending voice signals over the Internet is called Voice over IP or VoIP.</p> <p>H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service.</p> <p>H.323 is transported primarily over TCP, using the default port number 1720.</p>
TFTP	<p>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).</p>

5.3 Bandwidth Management Wizard Setup

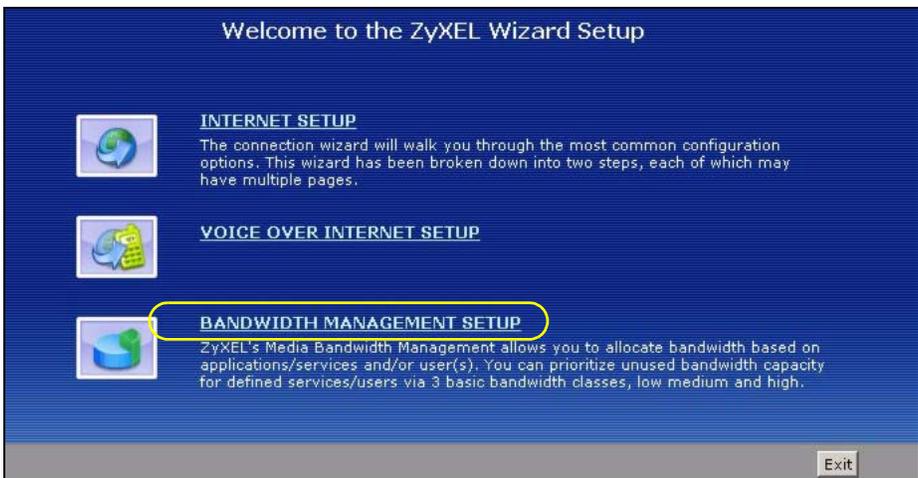
- 1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon () in the top right corner of the web configurator to display the wizard main screen.

Figure 28 Select a Mode



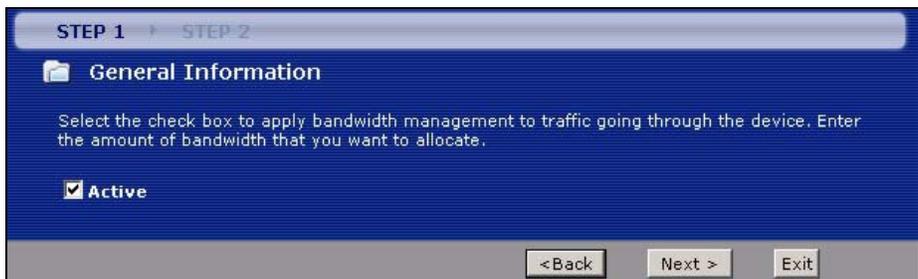
2 Click **BANDWIDTH MANAGEMENT SETUP**.

Figure 29 Wizard: Welcome



3 Activate bandwidth management and select to allocate bandwidth to packets based on the packet size or services.

Figure 30 Bandwidth Management Wizard: General Information



The following fields describe the label in this screen.

Table 14 Bandwidth Management Wizard: General Information

LABEL	DESCRIPTION
Active	Select the Active check box to have the ZyXEL Device apply bandwidth management to traffic going out through the ZyXEL Device's WAN or LAN port. Select Auto Classifier to automatically allocate bandwidth to packets based on the packet size or Services Setup to allocate bandwidth based on the service requirements.
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.

- If you select **Service Setup**, use the second wizard screen to select the services that you want to apply bandwidth management and select the priorities that you want to apply to the services listed.

Figure 31 Bandwidth Management Wizard: Service Configuration



The following table describes the labels in this screen.

Table 15 Bandwidth Management Wizard: Service Configuration

LABEL	DESCRIPTION
Active	Select Active to enable bandwidth management for service specified traffic. Select an entry's Active check box to turn on bandwidth management for the service/application.
Service	These fields display the services names.

Table 15 Bandwidth Management Wizard: Service Configuration

LABEL	DESCRIPTION
Priority	<p>Select High, Mid or Low priority for each service to have your ZyXEL Device use a priority for traffic that matches that service.</p> <p>A service with High priority is given as much bandwidth as it needs.</p> <p>If you select services as having the same priority, then bandwidth is divided equally amongst those services.</p> <p>Services not specified in bandwidth management are allocated bandwidth after all specified services receive their bandwidth requirements.</p> <p>If the rules set up in this wizard are changed in Advanced, Bandwidth MGMT, Rule Setup, then the service priority radio button will be set to User Configured.</p> <p>The Advanced, Bandwidth MGMT, Rule Setup screen allows you to edit these rule configurations.</p>
Back	Click Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Exit	Click Exit to close the wizard screen without saving your changes.

- 5 Follow the on-screen instructions and click **Finish** to complete the wizard setup and save your configuration.

Figure 32 Bandwidth Management Wizard: Complete

CHAPTER 6

Status Screens

Use the **Status** screens to look at the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and unregister SIP accounts. The **Status** screen also provides detailed information from Any IP and DHCP and statistics from VoIP, bandwidth management, and traffic.

6.1 Status Screen

Click **Status** to open this screen.

Figure 33 Status Screen

The screenshot displays the Status Screen with a 'Refresh Interval' dropdown set to 'None' and an 'Apply' button. The screen is divided into several sections:

- Device Information:**
 - Host Name:
 - Model Number: P-2602RL-D1A
 - MAC Address: 00:13:49:00:00:01
 - ZyNOS Firmware Version: [V3.40\(ADP.0\)b4 | 03/08/2006](#)
 - DSL Firmware Version: TI AR7 05.01.03.00
 - WAN Information:
 - DSL Mode: NORMAL
 - IP Address: [0.0.0.0](#)
 - IP Subnet Mask: 0.0.0.0
 - Default Gateway: 0.0.0.0
 - VPI/VCI: 8/35
 - LAN Information:
 - IP Address: [192.168.1.1](#)
 - IP Subnet Mask: 255.255.255.0
 - DHCP: [Server](#)
 - Security:
 - Firewall: [Enabled](#)
 - Content Filter: [Disable](#)
- System Status:**
 - System Uptime: 0:05:08
 - Current Date/Time: 01/01/2000 00:10:05
 - System Mode: Routing / Bridging
 - CPU Usage: 5.97%
 - Memory Usage: 60%
- Interface Status:**

Interface	Status	Rate
DSL	Down	0 kbps / 0 kbps
LAN	Up	100M/Full Duplex
- Summary:**
 - [Client List](#)
 - [Bandwidth Status](#)
 - [VoIP Statistics](#)
 - [AnyIP Table](#)
 - [Packet Statistics](#)
- VoIP Status:**

Account	Registration	URI
SIP 1	Register Register Fail	ChangeMe@127.0.0.1
SIP 2	Register Inactive	ChangeMe@127.0.0.1

Each field is described in the following table.

Table 16 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Apply	Click this to update this screen immediately.
Device Information	
Host Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the Maintenance > System > General screen's System Name field.
Model Number	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
ZyNOS Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This field displays the current version of the device's DSL modem code.
WAN Information	
DSL Mode	This is the DSL standard that your ZyXEL Device is using.
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the wizard or WAN screen.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: Server - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. None - The ZyXEL Device is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
Security	
Firewall	This displays whether or not the ZyXEL Device's firewall is activated. Click this to go to the screen where you can change it.
Content Filter	This displays whether or not the ZyXEL Device's content filtering is activated. Click this to go to the screen where you can change it.
System Status	

Table 16 Status Screen

LABEL	DESCRIPTION
System Uptime	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (Maintenance > Tools > Restart), or when you reset it (see Section 2.1.2 on page 47).
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in Maintenance > System > Time Setting .
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management; see Chapter 16 on page 187).
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See Section 22.6 on page 241 , or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.
Status	For the DSL interface, this field displays Down (line is down), Up (line is up or connected) if you're using Ethernet encapsulation and Down (line is down), Up (line is up or connected), Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE encapsulation. This field indicates whether or not the ZyXEL Device is using the interface. For the LAN interface, this field displays Up when the ZyXEL Device is using the interface and Down when the ZyXEL Device is not using the interface.
Rate	For the LAN interface, this displays the port speed and duplex setting. For the DSL interface, it displays the downstream and upstream transmission rate.
Summary	
Client List	Click this link to view current DHCP client information. See Section 8.5 on page 104 .
AnyIP Table	Click this link to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the ZyXEL Device. See Section 6.2 on page 76 .
Bandwidth Status	Click this link to view the ZyXEL Device's bandwidth usage and allotments. See Section 16.9 on page 196 .
Packet Statistics	Click this link to view port status and packet specific statistics. See Section 6.3 on page 77 .
VoIP Statistics	Click this link to view statistics about your VoIP usage. See Section 6.4 on page 78 .
VoIP Status	
Account	This column displays each SIP account in the ZyXEL Device.

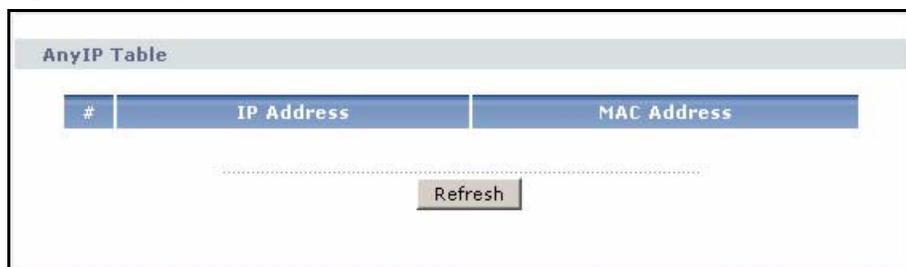
Table 16 Status Screen

LABEL	DESCRIPTION
Registration	<p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p>If the SIP account is already registered with the SIP server,</p> <ul style="list-style-type: none"> Click Unregister to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. The second field displays Registered. <p>If the SIP account is not registered with the SIP server,</p> <ul style="list-style-type: none"> Click Register to have the ZyXEL Device attempt to register the SIP account with the SIP server. The second field displays the reason the account is not registered. <p>Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Settings.</p> <p>Register Fail - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.</p>
URI	<p>This field displays the account number and service domain of the SIP account. You can change these in VoIP > SIP > SIP Settings.</p>

6.2 Any IP Table

Click **Status > AnyIP Table** to access this screen. Use this screen to view the IP address and MAC address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.

Figure 34 Any IP Table



Each field is described in the following table.

Table 17 Any IP Table

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.

Table 17 Any IP Table

LABEL	DESCRIPTION
MAC Address	This field displays the MAC address of the computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
Refresh	Click this to update this screen.

6.3 Packet Statistics

Click **Status > Packet Statistics** to access this 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 35 Packet Statistics

The screenshot displays the Packet Statistics screen with the following sections:

- System Monitor:**
 - System up Time: 15:45:54
 - Current Date/Time: 01/01/2000 15:57:05
 - CPU Usage: 5.21%
 - Memory Usage: 54%
- WAN Port Statistics:**
 - Link Status: Down
 - WAN IP Address: 0.0.0.0
 - Upstream Speed: 0 kbps
 - Downstream Speed: 0 kbps

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

Ethernet	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full Duplex	1440	1293	0

At the bottom, there is a **Poll Interval(s)** field set to 5 sec, with **Set Interval** and **Stop** buttons.

The following table describes the fields in this screen.

Table 18 Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
WAN Port Statistics	
Link Status	This is the status of your WAN link.

Table 18 Packet Statistics (continued)

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

6.4 VoIP Statistics

Click **Status > VoIP Statistics** to access this screen.

Figure 36 VoIP Statistics

SIP Status:							
Account	Registration	Last Registration	URI	Protocol	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP1	Register Fail	N/A	changeme@127.0.0.1	UDP	No	N/A	N/A
SIP2	Register Fail	N/A	changeme@127.0.0.1	UDP	No	N/A	N/A

Call Statistics:									
Phone	Hook	Status	Codec	Peer Number	Duration	TxPkts	RxPkts	Tx B/s	Rx B/s
Phone1	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone2	On	N/A	N/A	N/A	0:00:00	0	0	0	0

Poll Interval(s) : sec

Each field is described in the following table.

Table 19 VoIP Statistics

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.
Registration	This field displays the current registration status of the SIP account. You can change this in the Status screen. Registered - The SIP account is registered with a SIP server. Register Fail - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it. Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Settings .
Last Registration	This field displays the last time you successfully registered the SIP account. It displays N/A if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in VoIP > SIP > SIP Settings .
Protocol	This field displays the transport protocol the SIP account uses. SIP accounts always use UDP.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. It displays N/A if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. It displays N/A if the SIP account has never dialed a number.
Call Statistics	

Table 19 VoIP Statistics

LABEL	DESCRIPTION
Phone	This field displays each phone port in the ZyXEL Device.
Hook	This field indicates whether the phone is on the hook or off the hook. On - The phone is hanging up or already hung up. Off - The phone is dialing, calling, or connected.
Status	This field displays the current state of the phone call. N/A - There are no current VoIP calls, incoming calls or outgoing calls being made. DIAL - The callee's phone is ringing. RING - The phone is ringing for an incoming VoIP call. Process - There is a VoIP call in progress. DISC - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Duration	This field displays how long the current call has lasted.
Tx Pkts	This field displays the number of packets the ZyXEL Device has transmitted in the current call.
Rx Pkts	This field displays the number of packets the ZyXEL Device has received in the current call.
Tx B/s	This field displays how quickly the ZyXEL Device has transmitted packets in the current call. The rate is the average number of bytes transmitted per second.
Rx B/s	This field displays how quickly the ZyXEL Device has received packets in the current call. The rate is the average number of bytes transmitted per second.
Poll Interval(s)	Enter how often you want the ZyXEL Device to update this screen, and click Set Interval .
Set Interval	Click this to make the ZyXEL Device update the screen based on the amount of time you specified in Poll Interval .
Stop	Click this to make the ZyXEL Device stop updating the screen.

CHAPTER 7

WAN Setup

This chapter describes how to configure WAN settings.

7.1 WAN Overview

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

7.1.1 Encapsulation

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

7.1.1.1 ENET ENCAP

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

7.1.1.2 PPP over Ethernet

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 (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

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

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

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

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

7.1.1.3 PPPoA

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

7.1.1.4 RFC 1483

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

7.1.2 Multiplexing

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

7.1.2.1 VC-based Multiplexing

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

7.1.2.2 LLC-based Multiplexing

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

7.1.3 VPI and VCI

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

7.1.4 IP Address Assignment

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

7.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation

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

7.1.4.2 IP Assignment with RFC 1483 Encapsulation

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

7.1.4.3 IP Assignment with ENET ENCAP Encapsulation

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

7.1.5 Nailed-Up Connection (PPP)

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

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

7.1.6 NAT

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

7.2 Metric

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

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

- Normal route: designated by the ISP (see [Section 7.5 on page 86](#))
- Traffic-redirect route (see [Section 7.7 on page 91](#))
- WAN-backup route, also called dial-backup (see [Section 7.8 on page 93](#))

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

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

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above.

7.3 Traffic Shaping

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

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

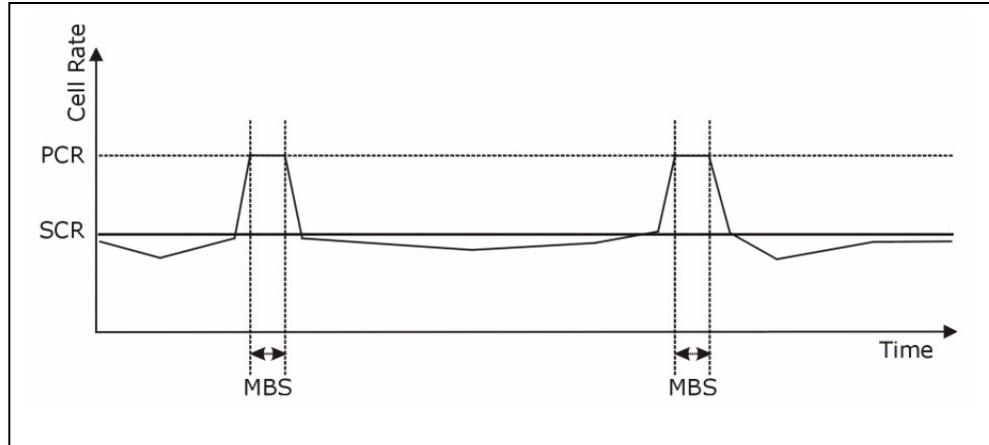
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

Figure 37 Example of Traffic Shaping



7.3.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

7.3.1.1 Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

7.3.1.2 Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

7.3.1.3 Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

7.4 Zero Configuration Internet Access

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

Zero configuration for Internet access is disable when

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

7.5 Internet Access Setup

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

See [Section 7.1 on page 81](#) for more information.

Figure 38 Internet Access Setup (PPPoE)

The following table describes the labels in this screen.

Table 20 Internet Access Setup

LABEL	DESCRIPTION
General	
Mode	Select Routing (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.

Table 20 Internet Access Setup (continued)

LABEL	DESCRIPTION
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	
IP Address	<p>This option is available if you select Routing in the Mode field.</p> <p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.</p> <p>Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field below.</p>
Subnet Mask (ENET ENCAP encapsulation only)	<p>Enter a subnet mask in dotted decimal notation.</p> <p>Refer to the appendix to calculate a subnet mask If you are implementing subnetting.</p>
Gateway IP address (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select ENET ENCAP in the Encapsulation field
DNS Server	
First DNS Server Second DNS Server Third DNS Server	<p>Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address).</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 only when the ISP uses IPCP DNS server extensions. 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 real DNS server learned through IPCP 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. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.

Table 20 Internet Access Setup (continued)

LABEL	DESCRIPTION
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session will not timeout.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.
Advanced Setup	Click this button to display the Advanced WAN Setup screen and edit more details of your WAN setup.

7.5.1 Advanced Internet Access Setup

To edit your ZyXEL Device's advanced WAN settings, click the **Advanced Setup** button in the **Internet Access Setup** screen. The screen appears as shown.

Figure 39 Advanced Internet Access Setup

The following table describes the labels in this screen.

Table 21 Advanced Internet Access Setup

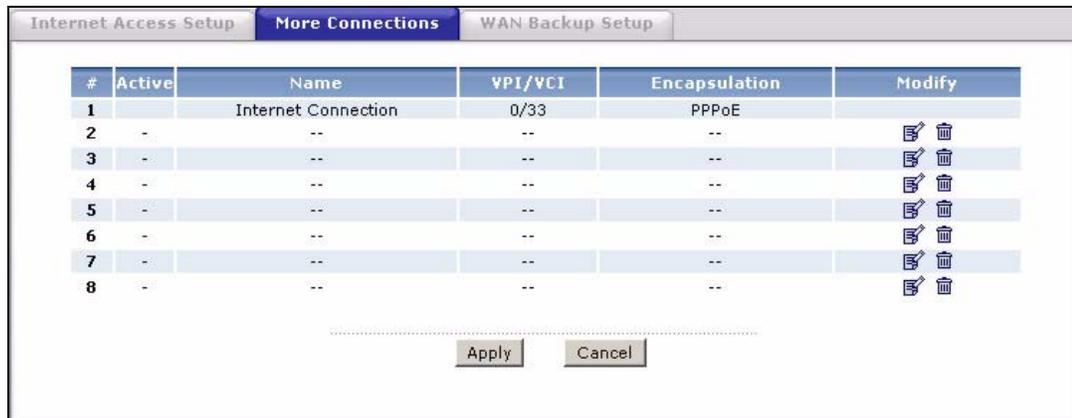
LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from None , Both , In Only and Out Only .
RIP Version	Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (IGMP-v1) and IGMP-v2 . Select None to disable it.
ATM QoS	

Table 21 Advanced Internet Access Setup (continued)

LABEL	DESCRIPTION
ATM QoS Type	Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR-RT (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select VBR-nRT (non real-time Variable Bit Rate) type for connections that do not require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Zero Configuration	This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode. Select Yes to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes. Select No to disable this feature. You must manually configure the ZyXEL Device for Internet access.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

7.6 WAN More Connections

The ZyXEL Device allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network > WAN > More Connections**. The screen differs by the encapsulation.

Figure 40 WAN More Connections

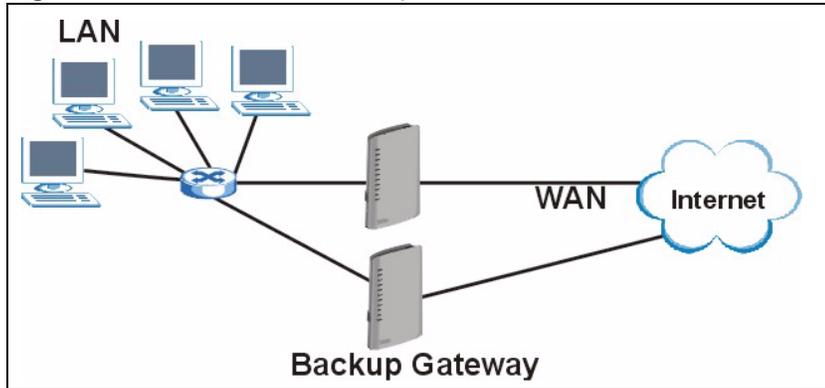
The following table describes the labels in this screen.

Table 22 Advanced Internet Access Setup

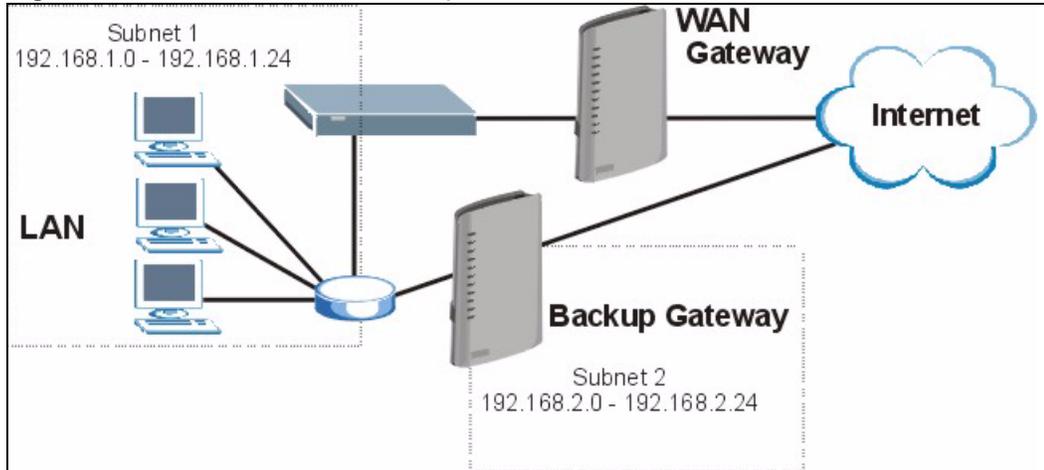
LABEL	DESCRIPTION
#	This is an index number indicating the number of the corresponding connection.
Active	This field indicates whether the connection is active or not.
Name	This is the name you gave to the Internet connection.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	Click the modify icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup. Click the delete icon to remove the Internet access setup from your connection list.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

7.7 Traffic Redirect

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

Figure 41 Traffic Redirect Example

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

Figure 42 Traffic Redirect LAN Setup

7.8 WAN Backup Setup

To configure your ZyXEL Device's WAN backup, click **Network > WAN > WAN Backup Setup**.

Internet Access Setup	More Connections	WAN Backup Setup
WAN Backup Setup		
Backup Type	DSL Link	
Check WAN IP Address 1	0.0.0.0	
Check WAN IP Address 2	0.0.0.0	
Check WAN IP Address 3	0.0.0.0	
Fail Tolerance	0	
Recovery Interval	0 sec	
Timeout	0 sec	
Traffic Redirect		
<input type="checkbox"/> Active Traffic Redirect		
Metric	15	
Backup Gateway	0.0.0.0	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

The following table describes the labels in this screen.

Table 23 WAN Backup Setup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select DSL Link to have the ZyXEL Device check if the connection to the DSLAM is up. Select ICMP to have the ZyXEL Device periodically ping the IP addresses configured in the Check WAN IP Address fields.
Check WAN IP Address1-3	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). Note: If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the Check WAN IP Address field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the Check WAN IP Address field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the Fail Tolerance field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.
Active Traffic Redirect	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 8

LAN Setup

This chapter describes how to configure LAN settings.

8.1 LAN Overview

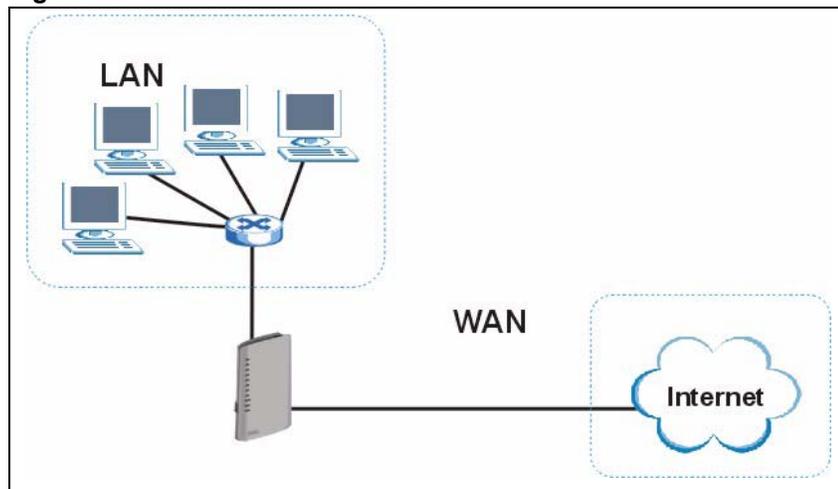
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 8.3 on page 101](#) to configure the LAN screens.

8.1.1 LANs, WANs and the ZyXEL Device

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

Figure 43 LAN and WAN IP Addresses



8.1.2 DHCP Setup

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

8.1.2.1 IP Pool Setup

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

8.1.3 DNS Server Address

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

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

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

If you set the router to be a DNS relay, it tells the DHCP clients that the device itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

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

8.1.4 DNS Server Address Assignment

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

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in the **DHCP Setup** screen.
- The ZyXEL Device acts as a DNS proxy when the **DNS Server** field is set to **DNS Relay** in the **DHCP Setup** screen.

8.2 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.

8.2.1 IP Address and Subnet Mask

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

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

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

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

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

8.2.1.1 Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

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

8.2.2 RIP Setup

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

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

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

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

8.2.3 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.

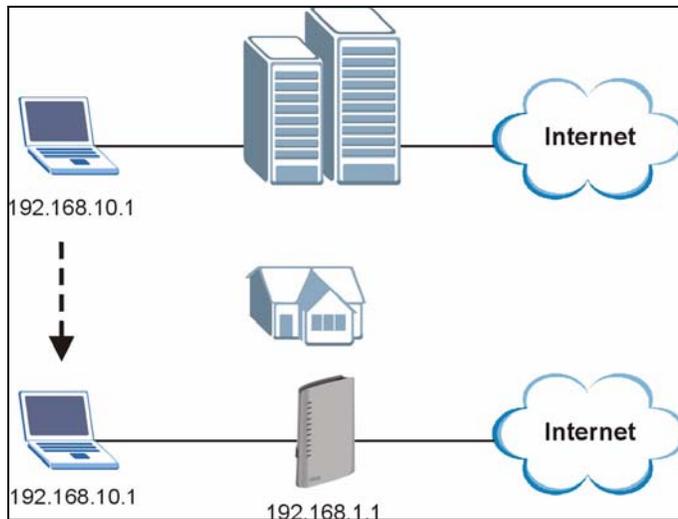
The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on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

8.2.4 Any IP

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

With the Any IP feature and NAT enabled, the ZyXEL Device allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the ZyXEL Device and access the Internet.

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

Figure 44 Any IP Example

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

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

8.2.4.1 How Any IP Works

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

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

- 1** When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.
- 2** When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
- 3** The ZyXEL Device receives the ARP request and replies to the computer with its own MAC address.
- 4** The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the ZyXEL Device.
- 5** When the ZyXEL Device receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

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

8.3 Configuring LAN IP

Click **Network > LAN** to open the **IP** screen. See [Section 8.1 on page 95](#) for background information.

Figure 45 LAN IP

The following table describes the fields in this screen.

Table 24 LAN IP

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.
Advanced Setup	Click this button to display the Advanced LAN Setup screen and edit more details of your LAN setup.

8.3.1 Configuring Advanced LAN Setup

To edit your ZyXEL Device's advanced LAN settings, click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

Figure 46 Advanced LAN Setup

The following table describes the labels in this screen.

Table 25 Advanced LAN Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from None , Both , In Only and Out Only .
RIP Version	Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (IGMP-v1) and IGMP-v2 . Select None to disable it.
Any IP Setup	Select the Active check box to enable the Any IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyXEL Device's LAN IP address can connect to the ZyXEL Device or access the Internet through the ZyXEL Device.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP 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.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

8.4 DHCP Setup

Click **Network > DHCP Setup** to open this screen. Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

Figure 47 DHCP Setup

The following table describes the labels in this screen.

Table 26 DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. If you select Server the ZyXEL Device provides TCP/IP configuration for the clients. When set as a server, fill in the IP Pool Starting Address and Pool Size fields. If you select Relay the ZyXEL Device forwards TCP/IP configuration from an alternate DHCP server. Select None to stop the ZyXEL Device from acting as a DHCP server. When you select None , you must have another DHCP server on your LAN, or else the computers must be manually configured.
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.
DNS Server	
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.

Table 26 DHCP Setup

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	<p>Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address).</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 only when the ISP uses IPCP DNS server extensions. 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 real DNS server learned through IPCP 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. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. 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.
Cancel	Click Cancel to begin configuring this screen afresh.

8.5 LAN Client List

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

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.

Click **Network > LAN > Client List** to open the following screen. Use this screen to change your ZyXEL Device's static DHCP settings.

Figure 48 LAN Client List

The screenshot shows a web interface for DHCP configuration. At the top, there are tabs for 'IP', 'DHCP Setup', 'Client List', and 'IP Alias'. The 'Client List' tab is active. Below the tabs is a 'DHCP Client Table' section. It contains two input fields: 'IP Address' with the value '192.168.1.66' and 'MAC Address' with the value 'AA:BB:CC:EE:EE:EE', followed by an 'Add' button. Below these is a table with the following data:

#	Status	Host Name	IP Address	MAC Address	Reserve	Modify
1		IBM1	192.168.1.33	11:22:33:44:55:66	<input checked="" type="checkbox"/>	
2			192.168.1.34	AA:BB:CC:DD:EE:FF	<input checked="" type="checkbox"/>	
3		HP	192.168.1.99	AA:BB:CC:KK:FF:GG	<input type="checkbox"/>	

At the bottom of the table area are three buttons: 'Apply', 'Reset', and 'Cancel'.

The following table describes the labels in this screen.

Table 27 LAN Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click Add to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
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 the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table. After you click Apply , the MAC address and IP address also display in the LAN Static DHCP screen (where you can edit them).
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.
Refresh	Click Refresh to reload the DHCP table.

8.6 LAN IP Alias

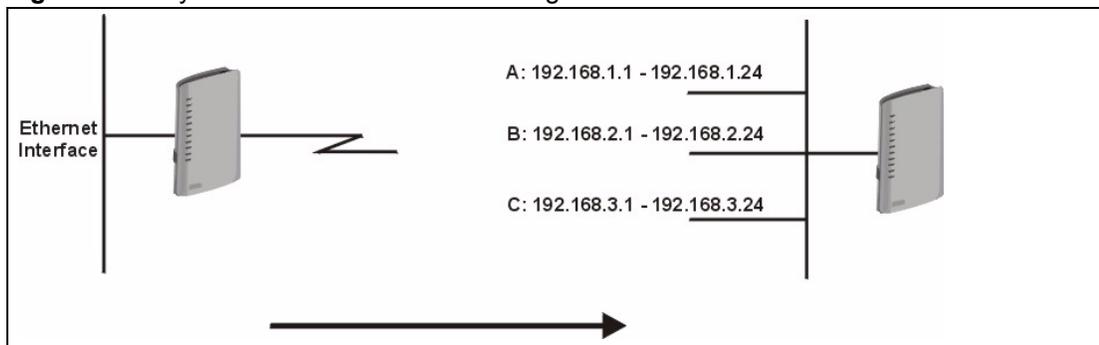
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Note: Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

Figure 49 Physical Network & Partitioned Logical Networks



Click **Network > LAN > IP Alias** to open the following screen. Use this screen to change your ZyXEL Device's IP alias settings.

Figure 50 LAN IP Alias

The screenshot shows the 'IP Alias' configuration page. It has tabs for 'IP', 'DHCP Setup', 'Client List', and 'IP Alias'. The page is divided into two sections: 'IP Alias 1' and 'IP Alias 2'. Each section has a checkbox to enable the alias, followed by input fields for 'IP Address' and 'IP Subnet Mask', and dropdown menus for 'RIP Direction' and 'RIP Version'. At the bottom, there are 'Apply' and 'Cancel' buttons.

IP Alias	IP Address	IP Subnet Mask	RIP Direction	RIP Version
IP Alias 1	0.0.0.0	0.0.0.0	None	N/A
IP Alias 2	0.0.0.0	0.0.0.0	None	N/A

The following table describes the labels in this screen.

Table 28 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. Alternatively, click the right mouse button to copy and/or paste the IP address.
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.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the ZyXEL Device will broadcast its routing table periodically. When set to Both or In Only , it will incorporate the RIP information that it receives; when set to None , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The RIP Version field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 9

Network Address Translation (NAT) Screens

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

9.1 NAT Overview

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

9.1.1 NAT Definitions

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

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

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

Table 29 NAT Definitions

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

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

9.1.2 What NAT Does

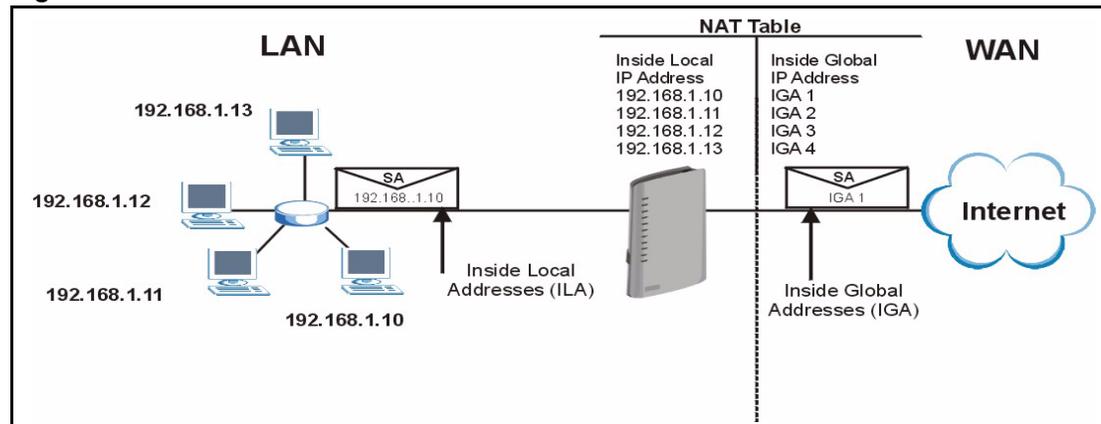
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 30 on page 112](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

9.1.3 How NAT Works

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

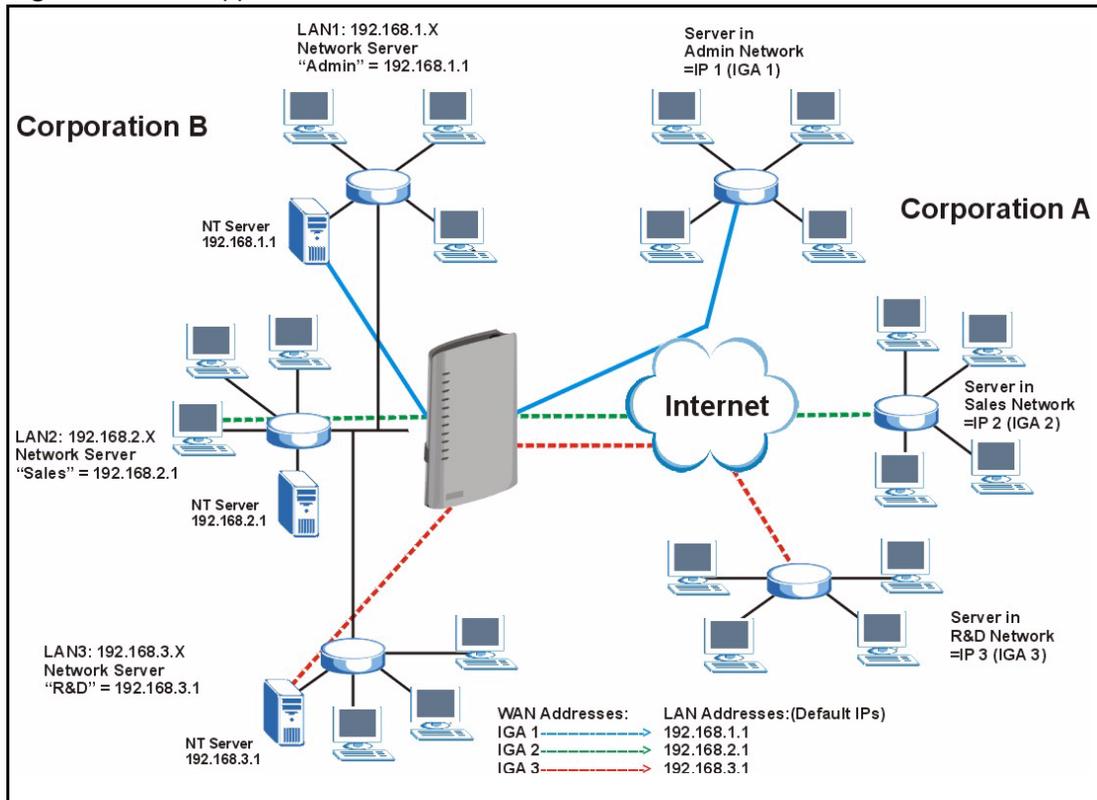
Figure 51 How NAT Works



9.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Aliases) behind the ZyXEL Device can communicate with three distinct WAN networks.

Figure 52 NAT Application With IP Alias



9.1.5 NAT Mapping Types

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

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

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

The following table summarizes these types.

Table 30 NAT Mapping Types

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

9.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 30 on page 112](#).

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

9.3 NAT General Setup

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device. Click **Network > NAT** to open the following screen.

Figure 53 NAT General

The following table describes the labels in this screen.

Table 31 NAT General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Max NAT/ Firewall Session Per User	When computers use peer to peer applications, such as file sharing applications, they need to establish 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 client computers 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 exhausting all of the available NAT sessions.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.4 Port Forwarding

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

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

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

9.4.1 Default Server IP Address

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

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

9.4.2 Port Forwarding: Services and Port Numbers

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

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

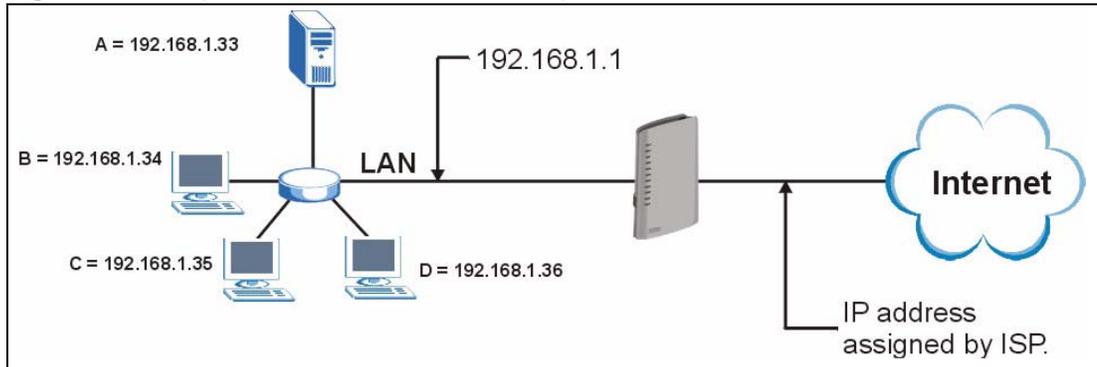
Table 32 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

9.4.3 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 54 Multiple Servers Behind NAT Example



9.5 Configuring Port Forwarding

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

Click **Network > NAT > Port Forwarding** to open the following screen.

See [Table 50 on page 152](#) for port numbers commonly used for particular services.

Figure 55 Port Forwarding

The screenshot shows the 'Port Forwarding' configuration screen. The 'Default Server Setup' section has 'Default Server' set to 0.0.0.0. The 'Port Forwarding' section has 'Service Name' set to WWW and 'Server IP Address' set to 0.0.0.0. Below this is a table with columns: #, Active, Service Name, Start Port, End Port, Server IP Address, and Modify. The table is currently empty. At the bottom are 'Apply' and 'Cancel' buttons.

#	Active	Service Name	Start Port	End Port	Server IP Address	Modify
---	--------	--------------	------------	----------	-------------------	--------

The following table describes the fields in this screen.

Table 33 Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
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 this screen. If you do not assign a Default Server IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	Click this check box to enable the rule.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previous configuration.

9.5.1 Port Forwarding Rule Edit

To edit a port forwarding rule, click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

Figure 56 Port Forwarding Rule Setup

The screenshot shows a web-based configuration window titled "Rule Setup". It contains the following elements:

- Active
- Service Name:
- Start Port:
- End Port:
- Server IP Address:

At the bottom of the window, there are three buttons: "Back", "Apply", and "Cancel".

The following table describes the fields in this screen.

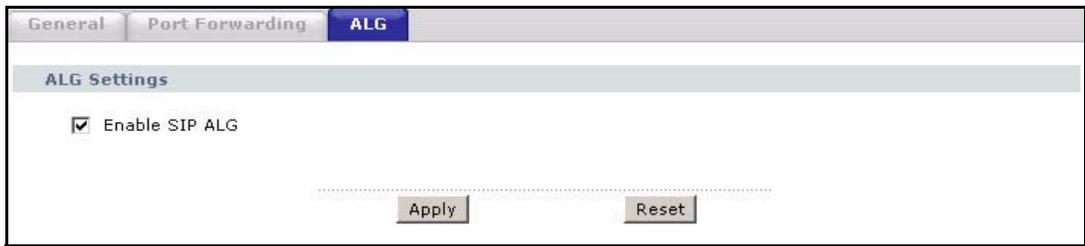
Table 34 Port Forwarding Rule Setup

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the End Port field. To forward a series of ports, enter the start port number here and the end port number in the End Port field.
End Port	Enter a port number in this field. To forward only one port, enter the port number again in the Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port field above.
Server IP Address	Enter the inside IP address of the server here.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

9.5.2 SIP ALG

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address.

Use this screen to enable and disable the SIP (VoIP) ALG in the ZyXEL Device. To access this screen, click **Network > NAT > ALG**.

Figure 57 Network > NAT > ALG

The screenshot shows the configuration page for ALG (Application Layer Gateway) settings. The page is titled 'ALG Settings' and is part of the 'Network > NAT > ALG' navigation path. The 'ALG' tab is selected. The main content area contains a single checkbox labeled 'Enable SIP ALG', which is currently checked. Below the checkbox, there are two buttons: 'Apply' and 'Reset'.

Each field is described in the following table.

Table 35 Network > NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to reset your settings to your last saved configuration.

CHAPTER 10

Voice

This chapter provides background information on VoIP and SIP and explains how to configure your device's voice settings.

10.1 Introduction to VoIP

VoIP is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

10.2 SIP

The Session Initiation Protocol (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 signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

10.2.1 SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

10.2.1.1 SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

10.2.1.2 SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

10.2.2 SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 36 SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	
	5. Dialogue (voice traffic)	
6. BYE	→	
	←	7. OK

- 1** A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
- 2** B sends a response indicating that the telephone is ringing.
- 3** B sends an OK response after the call is answered.
- 4** A then sends an ACK message to acknowledge that B has answered the call.
- 5** Now A and B exchange voice media (talk).
- 6** After talking, A hangs up and sends a BYE request.
- 7** B replies with an OK response confirming receipt of the BYE request and the call is terminated.

10.2.3 SIP Servers

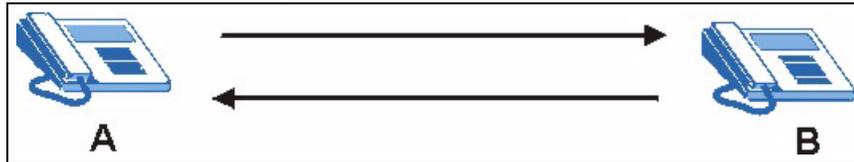
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

10.2.3.1 SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent to receive the call.

Figure 58 SIP User Agent

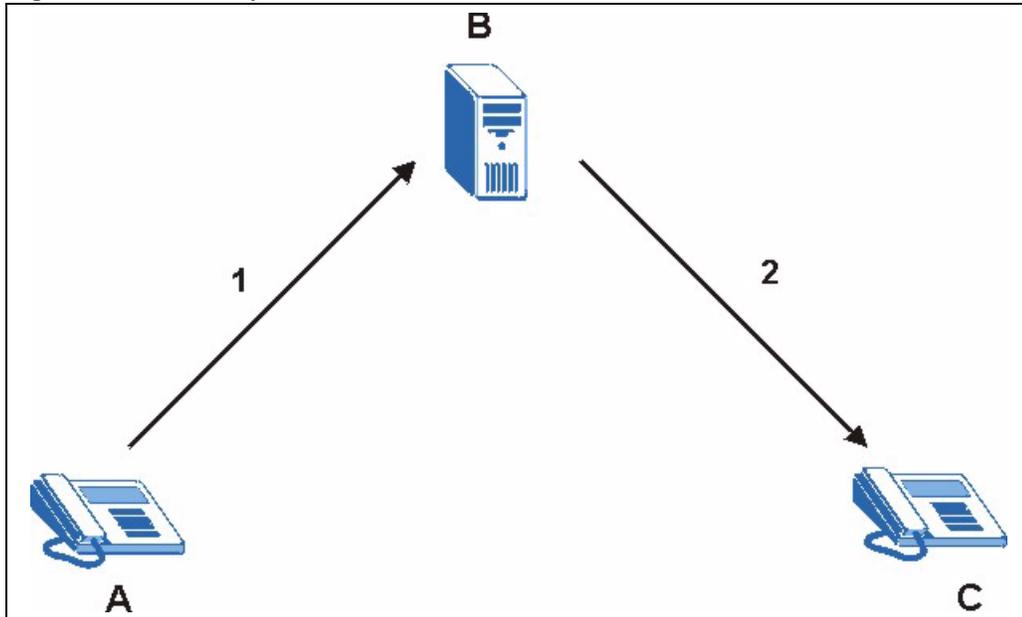


10.2.3.2 SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

- 1 The client device (A in the figure) sends a call invitation to the SIP proxy server (B).
- 2 The SIP proxy server forwards the call invitation to C.

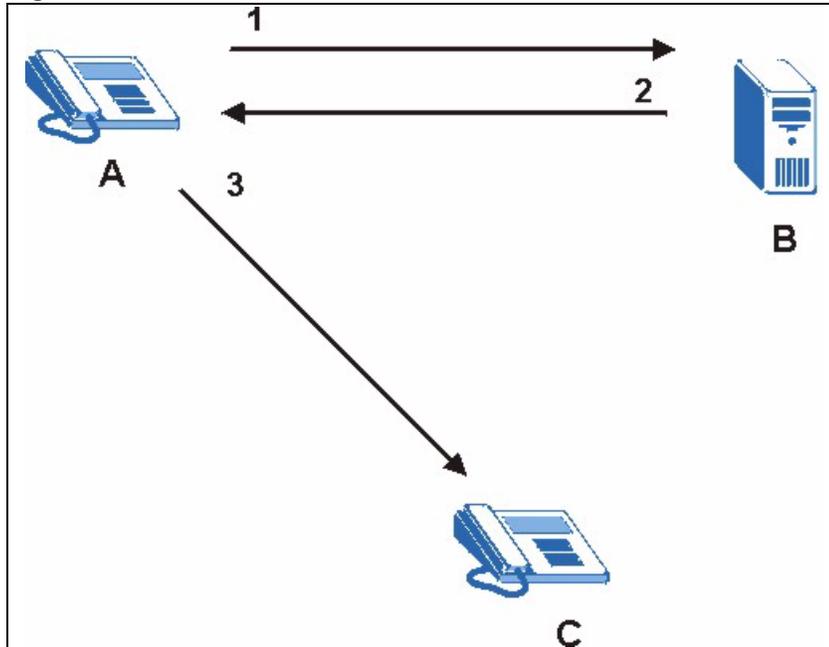
Figure 59 SIP Proxy Server

10.2.3.3 SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

- 1** Client device A sends a call invitation for C to the SIP redirect server (B).
- 2** The SIP redirect server sends the invitation back to A with C's IP address (or domain name).
- 3** Client device A then sends the call invitation to client device C.

Figure 60 SIP Redirect Server

10.2.3.4 SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

10.2.3.5 Multiple SIP Accounts

You can set up 2 SIP accounts on your ZyXEL Device and your ZyXEL Device is equipped with 2 phone ports. When 2 SIP accounts are configured, the ZyXEL Device uses SIP account 1 for both phone ports for your outgoing calls. The ZyXEL Device also directs calls coming in from both SIP accounts to both phone ports. You can configure a specific phone port, for example phone port 1, to only receive calls from a specific SIP account and make phone calls via a specific SIP account, for example SIP account 1. This is useful when you have different calling plans associated with your SIP accounts and want to manage your costs.

10.3 SIP Settings Screen

Use this screen to maintain basic information about each SIP account. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP > SIP Settings**.

Note: If you configure more than one SIP account, you need to configure **Analog Phone** settings in [Section 10.12 on page 134](#) to distinguish between them when you make and receive phone calls.

Figure 61 SIP > SIP Settings

Each field is described in the following table.

Table 37 SIP > SIP Settings

LABEL	DESCRIPTION
SIP Account	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.
SIP Settings	
Active SIP Account	Select this if you want the ZyXEL Device to use this account. Clear it if you do not want the ZyXEL Device to use this account.
Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
SIP Local Port	Enter the ZyXEL Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field.

Table 37 SIP > SIP Settings

LABEL	DESCRIPTION
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this SIP account. The Advanced SIP Setup screen appears.

10.3.1 RTP

When you make a VoIP call using SIP, the RTP (Real Time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

10.4 Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

10.5 Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The ZyXEL Device supports the following codecs.

10.5.1 G.711

G.711 is a Pulse Code Modulation (PCM) waveform codec. G.711 provides very good sound quality but requires 64kbps of bandwidth.

10.5.2 G.729

G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

10.6 PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.¹

10.7 MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message-waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

10.8 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the ZyXEL Device. The ZyXEL Device allows you to record custom tones for the **Caller Ringing Tone** and **On Hold Tone** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 38 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	120 seconds for all custom tones combined
Time per Individual Tone	20 seconds
Total Number of Tones Recordable	Ten You can record up to ten different custom tones but the total time must be 120 seconds or less. For example you could record up to ten 12-second tones or up to six 20-second tones.

10.8.0.1 Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

- 1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1101~1108 on your phone followed by the “#” key.
- 3 Play your desired music or voice recording into the receiver’s mouthpiece. Press the “#” key.

1. The ZyXEL Device does not support pulse dialing at the time of writing.

- 4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

10.8.0.2 Listening to Custom Tones

Do the following to listen to a custom tone:

- 1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1201~1208 followed by the “#” key to listen to the tone.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

10.8.0.3 Deleting Custom Tones

Do the following to delete a custom tone:

- 1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1301~1308 followed by the “#” key to delete the tone of your choice. Press 14 followed by the “#” key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

10.9 Advanced SIP Setup Screen

Click **VoIP > SIP > SIP Settings** to open the **SIP Settings** screen. Select a SIP account and click **Advanced Setup** to open the **Advanced SIP Setup** screen. Use this screen to maintain advanced settings for each SIP account.

Figure 62 VoIP > SIP Settings > Advanced

SIP Account : SIP1

SIP Server Settings

URL Type

Expiration Duration (20-65535) sec

Register Re-send timer (1-65535) sec

Session Expires (30-3600) sec

Min-SE (20-1800) sec

RTP Port Range

Start Port (1025-65535)

End Port (1025-65535)

Voice Compression

Primary Compression Type

Secondary Compression Type

Third Compression Type

DTMF Mode

Outbound Proxy

Enable

Server Address

Server Port (1025-65535)

MWI (Message Waiting Indication)

Enable

Expiration Time (1-65535) sec

Fax Option

G.711 Fax Passthrough T.38 Fax Relay

Call Forward

Call Forward Table

Caller Ringing

Enable

Caller Ringing Tone

On Hold

Enable

On Hold Tone

Each field is described in the following table.

Table 39 VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
SIP Account	This field displays the SIP account you see in this screen.
SIP Server Settings	
URL Type	<p>Select whether or not to include the SIP service domain name when the ZyXEL Device sends the SIP number.</p> <p>SIP - include the SIP service domain name</p> <p>TEL - do not include the SIP service domain name</p>
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The ZyXEL Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the ZyXEL Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the ZyXEL Device accepts.
RTP Port Range	
Start Port End Port	<p>Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.</p> <p>To enter one port number, enter the port number in the Start Port and End Port fields.</p> <p>To enter a range of ports,</p> <ul style="list-style-type: none"> • enter the port number at the beginning of the range in the Start Port field • enter the port number at the end of the range in the End Port field.
Voice Compression	<p>Select the type of voice coder/decoder (codec) that you want the ZyXEL Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps).</p> <ul style="list-style-type: none"> • G.711A is typically used in Europe. • G.711u is typically used in North America and Japan. <p>In contrast, G.729 only requires 8 kbps.</p> <p>The ZyXEL Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.</p>
Primary Compression Type	Select the ZyXEL Device's first choice for voice coder/decoder.
Secondary Compression Type	Select the ZyXEL Device's second choice for voice coder/decoder. Select None if you only want the ZyXEL Device to accept the first choice.
Third Compression Type	Select the ZyXEL Device's third choice for voice coder/decoder. Select None if you only want the ZyXEL Device to accept the first or second choice.

Table 39 VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
DTMF Mode	<p>Control how the ZyXEL Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.</p> <p>RFC 2833 - send the DTMF tones in RTP packets</p> <p>PCM - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones.</p> <p>SIP INFO - send the DTMF tones in SIP messages</p>
Outbound Proxy	
Active	<p>Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the ZyXEL Device to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).</p>
Server Address	<p>Enter the IP address or domain name of the SIP outbound proxy server.</p>
Server Port	<p>Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.</p>
MWI (Message Waiting Indication)	
Enable	<p>Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.</p>
Expiration Time	<p>Keep the default value, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the ZyXEL Device subscribes to the service. Before this time passes, the ZyXEL Device automatically subscribes again.</p>
Fax Option	<p>This field controls how the ZyXEL Device handles fax messages.</p>
G.711 Fax Passthrough	<p>Select this if the ZyXEL Device should use G.711 to send fax messages. The peer devices must also use G.711.</p>
T.38 Fax Relay	<p>Select this if the ZyXEL Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have interoperability problems. The peer devices must also use T.38.</p>
Call Forward	
Call Forward Table	<p>Select which call forwarding table you want the ZyXEL Device to use for incoming calls. You set up these tables in VoIP > Phone Book > Incoming Call Policy.</p>
Caller Ringing	
Enable	<p>Select the check box if you want to specify what tone people hear when they call you. The ZyXEL Device provides a default tone, but you can add additional tones using IVR. See Section 10.8 on page 126 for more information.</p>
Caller Ringing Tone	<p>Select the tone you want people to hear when they call you. You should setup these tones using IVR first. See Section 10.8 on page 126 for more information.</p>
On Hold	
Enable	<p>Select the check box if you want to specify what tone people hear when you put them on hold. The ZyXEL Device provides a default tone, but you can add additional tones using IVR. See Section 10.8 on page 126 for more information.</p>
On Hold Tone	<p>Select the tone you want people to hear when you put them on hold. You should setup these tones using IVR first. See Section 10.8 on page 126 for more information.</p>

Table 39 VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
Back	Click this to return to the SIP Settings screen without saving your changes.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.10 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

10.10.1 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

10.10.2 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.¹

10.10.2.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

1. The ZyXEL Device does not support DiffServ at the time of writing.

Figure 63 DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)
-----------------	-------------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

10.10.3 VLAN

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your ZyXEL Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the ZyXEL Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

10.10.4 SIP QoS Screen

Use this screen to maintain ToS and VLAN settings for the ZyXEL Device. To access this screen, click **VoIP > SIP > QoS**.

Figure 64 SIP > QoS

SIP Settings		QoS
TOS		
SIP TOS Priority Setting	<input type="text" value="5"/>	(0~255)
RTP TOS Priority Setting	<input type="text" value="5"/>	(0~255)
VLAN Tagging		
<input type="checkbox"/> Voice VLAN ID	<input type="text" value="0"/>	(0~4095)
<input type="button" value="Apply"/>		<input type="button" value="Reset"/>

Each field is described in the following table.

Table 40 SIP > QoS

LABEL	DESCRIPTION
SIP TOS Priority Setting	Enter the priority for SIP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to voice traffic that it transmits.
RTP TOS Priority Setting	Enter the priority for RTP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to RTP traffic that it transmits.

Table 40 SIP > QoS

LABEL	DESCRIPTION
Voice VLAN ID	Select this if the ZyXEL Device has to be a member of a VLAN to communicate with the SIP server. Ask your network administrator, if you are not sure. Enter the VLAN ID provided by your network administrator in the field on the right. Your LAN and gateway must be configured to use VLAN tags. Otherwise, clear this field.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.11 Phone

You can configure the volume, echo cancellation and VAD settings for each individual phone port on the ZyXEL Device. You can also select which SIP account to use for making outgoing calls.

10.11.1 PSTN Line (“L” Models only)

With PSTN line you can make and receive regular PSTN phone calls. Use a prefix number to make a regular call. When the device does not have power, you can make regular calls without dialing a prefix number.

You can also use the **PSTN Line** screen to specify phone numbers that should always use the regular phone service (without having to dial a prefix number). Do this for emergency numbers (like those for contacting police, fire or emergency medical services).

Note: When the ZyXEL Device does not have power, only the phone connected to the **PHONE 2** port can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.

10.11.2 Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the ZyXEL Device reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

10.11.3 Comfort Noise Generation

When using VAD, the ZyXEL Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

10.11.4 Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

10.12 Analog Phone

Use this screen to control which SIP accounts and PSTN line each phone uses. To configure your analog phone settings, click **VoIP > Phone > Analog Phone**.

Figure 65 Phone > Analog Phone

Each field is described in the following table.

Table 41 Phone > Analog Phone

LABEL	DESCRIPTION
Phone Port Settings	Select the phone port you want to see in this screen. If you change this field, the screen automatically refreshes.
Outgoing Call Use	
SIP1	Select this if you want this phone port to use the SIP1 account when it makes calls. If you select both SIP accounts, the ZyXEL Device tries to use SIP2 first.
SIP2	Select this if you want this phone port to use the SIP2 account when it makes calls. If you select both SIP accounts, the ZyXEL Device tries to use SIP2 first.
Incoming Call apply to	
SIP1	Select this if you want to receive phone calls for the SIP1 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
SIP2	Select this if you want to receive phone calls for the SIP2 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.

Table 41 Phone > Analog Phone

LABEL	DESCRIPTION
PSTN Line ("L" models only)	Select this if you want to receive phone calls from the PSTN line (that do not use the Internet) on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls. Note: When the ZyXEL Device does not have power, only the phone connected to the PHONE 2 port can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this phone port. The Advanced Analog Phone Setup screen appears.

10.13 Advanced Analog Phone Setup Screen

Use this screen to edit advanced settings for each phone port. To access this screen, click **Advanced Setup** in **VoIP > Phone > Analog Phone**.

Figure 66 Phone > Analog Phone > Advanced

Each field is described in the following table.

Table 42 Phone > Analog Phone > Advanced

LABEL	DESCRIPTION
Analog Phone	This field displays the phone port you see in this screen.
Voice Volume Control	

Table 42 Phone > Analog Phone > Advanced

LABEL	DESCRIPTION
Speaking Volume	Enter the loudness that the ZyXEL Device uses for speech that it sends to the peer device. -1 is the quietest, and 1 is the loudest.
Listening Volume	Enter the loudness that the ZyXEL Device uses for speech that it receives from the peer device. -1 is the quietest, and 1 is the loudest.
Echo Cancellation	
G.168 Active	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Dialing Interval Select	
Dialing Interval Select	Enter the number of seconds the ZyXEL Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select Active Immediate Dial in VoIP > Phone > Common , you can press the pound key (#) to tell the ZyXEL Device to make the phone call immediately, regardless of this setting.
VAD Support	Select this if the ZyXEL Device should stop transmitting when you are not speaking. This reduces the bandwidth the ZyXEL Device uses.
Back	Click this to return to the Analog Phone screen without saving your changes.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.13.1 Common Phone Settings Screen

Use this screen to activate and deactivate immediate dialing. To access this screen, click **VoIP > Phone > Common**.

Figure 67 Phone > Common

Each field is described in the following table.

Table 43 Phone > Common

LABEL	DESCRIPTION
Active Immediate Dial	Select this if you want to use the pound key (#) to tell the ZyXEL Device to make the phone call immediately, instead of waiting the number of seconds you selected in the Dialing Interval Select in VoIP > Phone > Analog Phone . If you select this, dial the phone number, and then press the pound key. The ZyXEL Device makes the call immediately, instead of waiting. You can still wait, if you want.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.14 Supplementary Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, ... are generally available from your VoIP service provider. The ZyXEL Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding (see [Section 10.18 on page 143](#))
- Three-Way Conference
- Internal Calls (see [Section 11.3 on page 147](#))

Note: To take full advantage of the supplementary phone services available through the ZyXEL Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

10.14.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the ZyXEL Device.

You can invoke all the supplementary services by using the flash key.

10.14.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 44 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

10.14.2.1 European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

10.14.2.2 European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.
Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.
Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.
Press the flash key and then “2”.

10.14.2.3 European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

10.14.2.4 European Three-Way Conference

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call.
- 3 When the second call is answered, press the flash key and press “3” to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

10.14.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 45 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

10.14.3.1 USA Call Hold

Call hold allows you to put a call (A) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller A and B by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

10.14.3.2 USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

10.14.3.3 USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

10.14.3.4 USA Three-Way Conference

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call (to party B).

- 3 When party B answers the second call, press the flash key to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.
- 6 If you want to go back to the three-way conversation, press the flash key again.
- 7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

10.15 Phone Region Screen

Use this screen to maintain settings that often depend on which region of the world the ZyXEL Device is in. To access this screen, click **VoIP > Phone > Region**.

Figure 68 VoIP > Phone > Region

Each field is described in the following table.

Table 46 VoIP > Phone > Region

LABEL	DESCRIPTION
Region Settings	Select the place in which the ZyXEL Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. Europe Type - use supplementary phone services in European mode USA Type - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.16 Speed Dial

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers.

10.16.1 Peer-to-Peer Calls

You can call another VoIP device directly without going through a SIP server. You must set up a speed dial entry in the phone book in order to do this. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The ZyXEL Device sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

You do not need to configure a SIP account on the ZyXEL Device in order to make a peer-to-peer VoIP call.

10.17 Speed Dial Screen

You have to create speed-dial entries if you want to make peer-to-peer calls or call SIP numbers that use letters. You can also create speed-dial entries for frequently-used SIP phone numbers. Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. To access this screen, click **VoIP > Phone Book > Speed Dial**.

Figure 69 Phone Book > Speed Dial

Each field is described in the following table.

Table 47 Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
Speed Dial	Select the speed-dial number you want to use for this phone number.

Table 47 Phone Book > Speed Dial

LABEL	DESCRIPTION
Number	Enter the SIP number you want the ZyXEL Device to call when you dial the speed-dial number.
Name	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Type	Select Use Proxy if you want to use one of your SIP accounts to call this phone number. Select Non-Proxy (Use IP or URL) if you want to use a different SIP server or if you want to make a peer-to-peer call. In this case, enter the IP address or domain name of the SIP server or the other party in the field below.
Add	Click this to use the information in the Speed Dial section to update the Speed Dial Phone Book section.
Speed Dial Phone Book	Use this section to look at all the speed-dial entries and to erase them.
Speed Dial	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the ZyXEL Device calls when you dial the speed-dial number.
Name	This field displays the name of the party you call when you dial the speed-dial number.
Destination	This field is blank, if the speed-dial entry uses one of your SIP accounts. Otherwise, this field shows the IP address or domain name of the SIP server or other party. (This field corresponds with the Type field in the Speed Dial section.)
Modify	Use this field to edit or erase the speed-dial entry. Click the Edit icon to copy the information for this speed-dial entry into the Speed Dial section, where you can change it. Click the Remove icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

10.18 Incoming Call Policy Screen

Use this screen to maintain rules for handling incoming calls. You can block, redirect, or accept them. To access this screen, click **VoIP > Phone Book > Incoming Call Policy**.

Figure 70 Phone Book > Incoming Call Policy

You can create two sets of call-forwarding rules. Each one is stored in a call-forwarding table. Each field is described in the following table.

Table 48 Phone Book > Incoming Call Policy

LABEL	DESCRIPTION
Table Number	Select the call-forwarding table you want to see in this screen. If you change this field, the screen automatically refreshes.
Forward to Number Setup	The ZyXEL Device checks these rules, in the order in which they appear, after it checks the rules in the Advanced Setup section.
Unconditional Forward to Number	Select this if you want the ZyXEL Device to forward all incoming calls to the specified phone number, regardless of other rules in the Forward to Number section. Specify the phone number in the field on the right.
Busy Forward to Number	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
No Answer Forward to Number	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the call is unanswered. (See No Answer Waiting Time .) Specify the phone number in the field on the right.
No Answer Waiting Time	This field is used by the No Answer Forward to Number feature and No Answer conditions below. Enter the number of seconds the ZyXEL Device should wait for you to answer an incoming call before it considers the call is unanswered.

Table 48 Phone Book > Incoming Call Policy

LABEL	DESCRIPTION
Advanced Setup	The ZyXEL Device checks these rules before it checks the rules in the Forward to Number section.
#	This field is a sequential value, and it is not associated with a specific rule. The sequence is important, however. The ZyXEL Device checks each rule in order, and it only follows the first one that applies.
Activate	Select this to enable this rule. Clear this to disable this rule.
Incoming Call Number	Enter the phone number to which this rule applies.
Forward to Number	Enter the phone number to which you want to forward incoming calls from the Incoming Call Number . You may leave this field blank, depending on the Condition .
Condition	<p>Select the situations in which you want to forward incoming calls from the Incoming Call Number, or select an alternative action.</p> <p>Unconditional - The ZyXEL Device immediately forwards any calls from the Incoming Call Number to the Forward to Number.</p> <p>Busy - The ZyXEL Device forwards any calls from the Incoming Call Number to the Forward to Number when your SIP account already has a call connected.</p> <p>No Answer - The ZyXEL Device forwards any calls from the Incoming Call Number to the Forward to Number when the call is unanswered. (See No Answer Waiting Time.)</p> <p>Block - The ZyXEL Device rejects calls from the Incoming Call Number.</p> <p>Accept - The ZyXEL Device allows calls from the Incoming Call Number. You might create a rule with this condition if you do not want incoming calls from someone to be forwarded by rules in the Forward to Number section.</p>
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.19 PSTN Line Screen

Use this screen to set up the PSTN line you use to make regular phone calls. To access this screen, click **VoIP > PSTN Line > General**.

Figure 71 PSTN Line > General

Each field is described in the following table.

Table 49 PSTN Line > General

LABEL	DESCRIPTION
PSTN Line Pre-fix Number	Enter 1 - 7 numbers you dial before you dial the phone number, if you want to make a regular phone call while one of your SIP accounts is registered. These numbers tell the ZyXEL Device that you want to make a regular phone call.
Relay to PSTN Line	Enter phone numbers (for regular calls, not VoIP calls) that you want to dial without the prefix number. For example, you should enter emergency numbers. The number (1 - 9) is not a speed-dial number. It is just a sequential value that is not associated with any phone number.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

CHAPTER 11

Phone Usage

This chapter describes how to use a phone connected to your ZyXEL Device for basic tasks.

11.1 Dialing a Telephone Number

The **PHONE** LED turns green when your SIP account is registered. Dial a SIP number like “12345” on your phone’s keypad.

Use speed dial entries (see [Section 10.16 on page 141](#)) for peer-to-peer calls or SIP numbers that use letters. Dial the speed dial entry on your telephone’s keypad.

Use your VoIP service provider’s dialing plan to call regular telephone numbers.

11.2 Using Speed Dial to Dial a Telephone Number

After configuring the speed dial entry and adding it to the phonebook, press the speed dial entry’s key combination on your phone’s keypad.

11.3 Internal Calls

Press “#####” on your phone’s keypad to call the ZyXEL Device’s other phone port.

11.4 Checking the Device’s IP Address

Do the following to listen to the ZyXEL Device’s current IP address.

- 1 Pick up your phone’s receiver.
- 2 Press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 3 Press “5” followed by the # key.
- 4 Listen to the IP address and make a note of it.
- 5 Hang up the receiver.

11.5 Auto Firmware Upgrade

During auto-provisioning, the ZyXEL Device checks to see if there is a newer firmware version. If newer firmware is available, the ZyXEL Device plays a recording when you pick up your phone's handset.

Press “*99#” to upgrade the ZyXEL Device's firmware.

Press “#99#” to not upgrade the ZyXEL Device's firmware.

CHAPTER 12

Firewalls

This chapter gives some background information on firewalls and introduces the ZyXEL Device firewall.

12.1 Firewall Overview

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.

Refer to [Section 13.5 on page 164](#) to configure default firewall settings.

Refer to [Section 13.6 on page 165](#) to view firewall rules.

Refer to [Section 13.6.1 on page 167](#) to configure firewall rules.

Refer to [Section 13.6.2 on page 170](#) to configure a custom service.

Refer to [Section 13.8.3 on page 177](#) to configure firewall thresholds.

12.2 Types of Firewalls

There are three main types of firewalls:

- Packet Filtering Firewalls
- Application-level Firewalls
- Stateful Inspection Firewalls

12.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

12.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

12.2.3 Stateful Inspection Firewalls

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. See [Section 12.5 on page 155](#) for more information on stateful inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

12.3 Introduction to ZyXEL's Firewall

The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. 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 also has packet filtering capabilities.

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

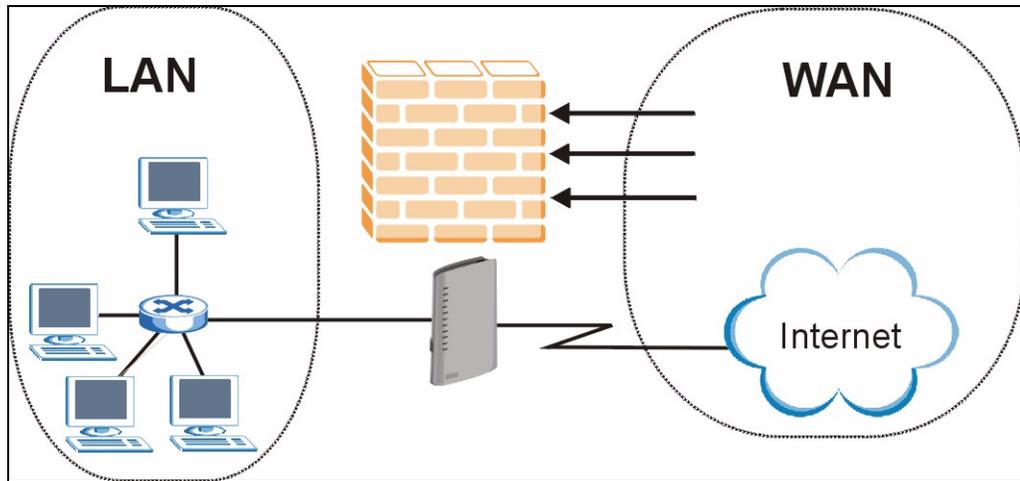
The ZyXEL Device has one DSL/ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

- The DSL/ISDN port connects 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” will not be allowed unless you configure remote management or create a firewall rule to allow a remote host to use a specific service.

12.3.1 Denial of Service Attacks

Figure 72 Firewall Application



12.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

12.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An “extension number”, called the “TCP port” or “UDP port” identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server “listens” on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 50 Common IP Ports

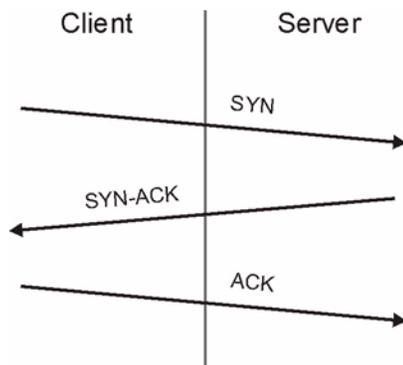
21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

12.4.2 Types of DoS Attacks

There are four types of DoS attacks:

- 1 Those that exploit bugs in a TCP/IP implementation.
- 2 Those that exploit weaknesses in the TCP/IP specification.
- 3 Brute-force attacks that flood a network with useless data.
- 4 IP Spoofing.
- 5 "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.
 - Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
 - Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.
- 6 Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

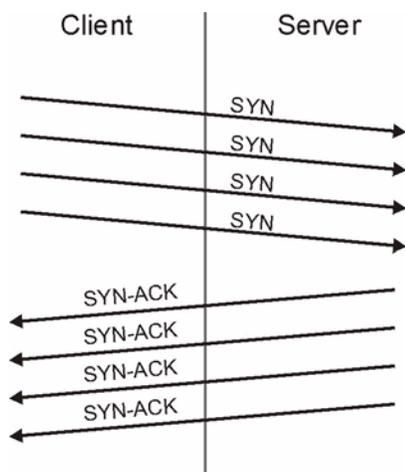
Figure 73 Three-Way Handshake



Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

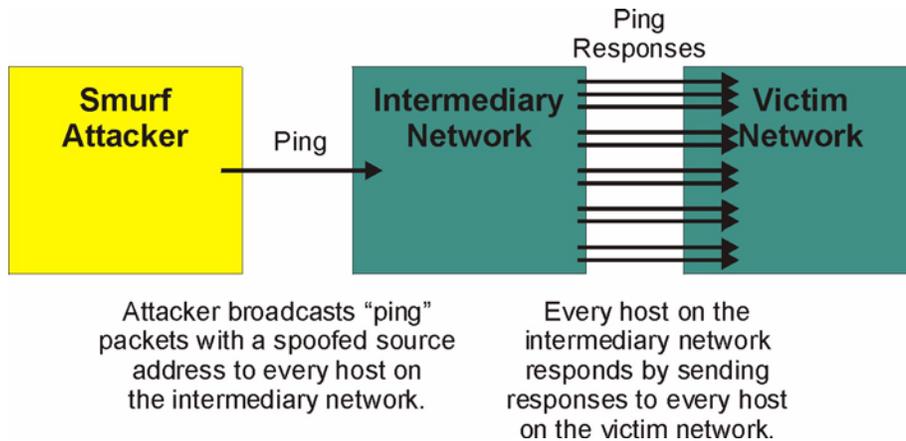
- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

Figure 74 SYN Flood



- In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.
- 7** A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 75 Smurf Attack



12.4.2.1 ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 51 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

12.4.2.2 Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 52 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
VE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 53 Legal SMTP Commands

AUTH	DATA	EHLO	ETRNL	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VERFY	

12.4.2.3 Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

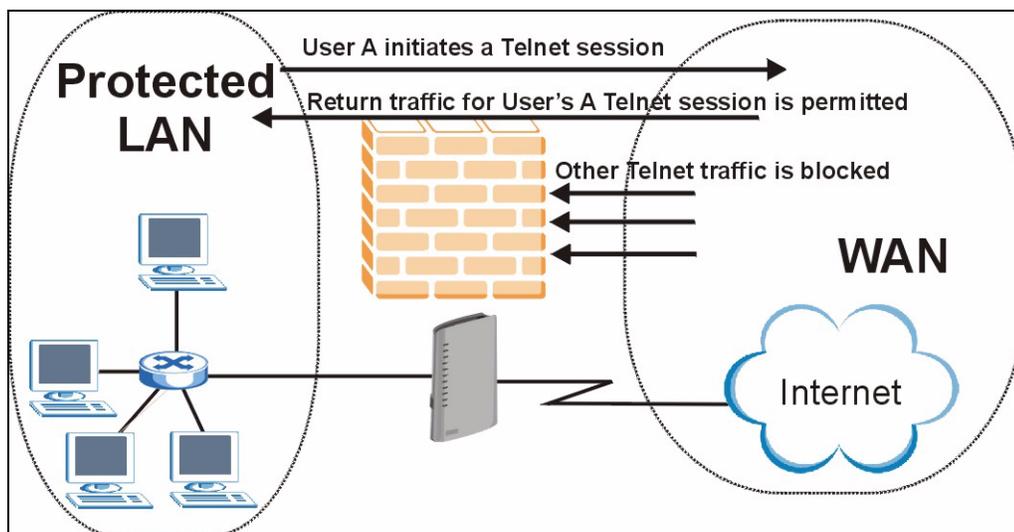
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyXEL Device blocks all IP Spoofing attempts.

12.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This "remembering" is called *saving the state*. When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The ZyXEL Device uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyXEL Device's stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

Figure 76 Stateful Inspection



The previous figure shows the ZyXEL Device's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

12.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

- 1 The packet travels from the firewall's LAN to the WAN.
- 2 The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
- 3 The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then the settings in the **Firewall General** screen determine the action for this packet.
- 4 Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
- 5 The outbound packet is forwarded out through the interface.
- 6 Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
- 7 The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
- 8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
- 9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

12.5.2 Stateful Inspection on Your ZyXEL Device

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.

- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyXEL Device itself (as with the "virtual connections" created for UDP and ICMP).

12.5.3 TCP Security

The ZyXEL Device uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyXEL Device receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

12.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyXEL Device is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

12.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyXEL Device inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these, it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's Custom Ports feature to do this.

12.6 Guidelines for Enhancing Security with Your Firewall

- Change the default password.
- Limit who can telnet into your router.
- 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.
- 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.
- Protect against IP spoofing by making sure the firewall is active.
- Keep the firewall in a secured (locked) room.

12.6.1 Security In General

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

- Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
- DSL or cable modem connections are “always-on” connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
- Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
- Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
- Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small “key” icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
- Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
- Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
- If you use “chat rooms” or IRC sessions, be careful with any information you reveal to strangers.
- If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.
- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

12.7 Packet Filtering Vs Firewall

Below are some comparisons between the ZyXEL Device’s filtering and firewall functions.

12.7.1 Packet Filtering:

- The router filters packets as they pass through the router’s interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

12.7.1.1 When To Use Filtering

- To block/allow LAN packets by their MAC addresses.
- To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
- To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- To block/allow IP trace route.

12.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

12.7.2.1 When To Use The Firewall

- To prevent DoS attacks and prevent hackers cracking your network.
- A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
- To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- The firewall performs better than filtering if you need to check many rules.
- Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

CHAPTER 13

Firewall Configuration

This chapter shows you how to enable and configure the ZyXEL Device firewall.

13.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyXEL Device has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. CLI commands provide limited configuration options and are only recommended for advanced users.

13.2 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ Router
- LAN to WAN
- WAN to LAN
- WAN to WAN/ Router

By default, the ZyXEL Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ Router
This allows computers on the LAN to manage the ZyXEL Device and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN

By default, the ZyXEL Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ Router

This prevents computers on the WAN from using the ZyXEL Device as a gateway to communicate with other computers on the WAN and/or managing the ZyXEL Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

Note: If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyXEL Device's default rules.

13.3 Rule Logic Overview

Note: Study these points carefully before configuring rules.

13.3.1 Rule Checklist

State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."

- 1 Is the intent of the rule to forward or block traffic?
- 2 What direction of traffic does the rule apply to?
- 3 What IP services will be affected?
- 4 What computers on the LAN are to be affected (if any)?
- 5 What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

13.3.2 Security Ramifications

- 1 Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:
- 2 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 3 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

- 4 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 5 Does this rule conflict with any existing rules?
- 6 Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

13.3.3 Key Fields For Configuring Rules

13.3.3.1 Action

Should the action be to **Drop**, **Reject** or **Permit**?

Note: “Drop” means the firewall silently discards the packet. “Reject” means the firewall discards packets and sends an ICMP destination-unreachable message to the sender.

13.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See [Appendix 28 on page 293](#) for more information on predefined services.

13.3.3.3 Source Address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

13.3.3.4 Destination Address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

13.4 Connection Direction

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/ Router, WAN to WAN/ Router and DMZ to DMZ/ Router rules apply to packets coming in on the associated interface (LAN, WAN or DMZ respectively). LAN to LAN/ Router means policies for LAN-to-ZyXEL Device (the policies for managing the ZyXEL Device through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly, WAN to WAN/ Router and DMZ to DMZ/ Router policies apply in the same way to the WAN and DMZ ports.

13.4.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

13.4.2 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when a rule is matched in the **Edit Rule** screen (see [Figure 79 on page 168](#)). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen. Refer to [Chapter 21 on page 229](#) for details.

13.5 General Firewall Policy

Click **Security > Firewall** to display the following screen. Activate the firewall by selecting the **Active Firewall** check box as seen in the following screen.

Refer to [Section 12.1 on page 149](#) for more information.

Figure 77 Firewall: General

Packet Direction	Default Action	Log
WAN to LAN	Drop	<input checked="" type="checkbox"/>
LAN to WAN	Permit	<input checked="" type="checkbox"/>
WAN to WAN / Router	Drop	<input checked="" type="checkbox"/>
LAN to LAN / Router	Permit	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 54 Firewall: General

LABEL	DESCRIPTION
Active 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.
Bypass Triangle Route	<p>Select this check box to have the ZyXEL Device firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology.</p> <p>Note: Allowing asymmetrical routes may let traffic from the WAN go directly to a LAN computer without passing through the router. See Appendix G on page 299 for more on triangle route topology and how to deal with this problem.</p>
Packet Direction	<p>This is the direction of travel of packets (LAN to LAN / Router, LAN to WAN, WAN to WAN / Router, WAN to LAN).</p> <p>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, LAN to LAN / Router means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyXEL Device or the ZyXEL Device itself.</p>
Default Action	<p>Use the drop-down list boxes to select the default action that the firewall is take on packets that are traveling in the selected direction and do not match any of the firewall rules.</p> <p>Select Drop to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select Reject to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select Permit to allow the passage of the packets.</p>
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this button to display more information.
Basic...	Click this button to display less information.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

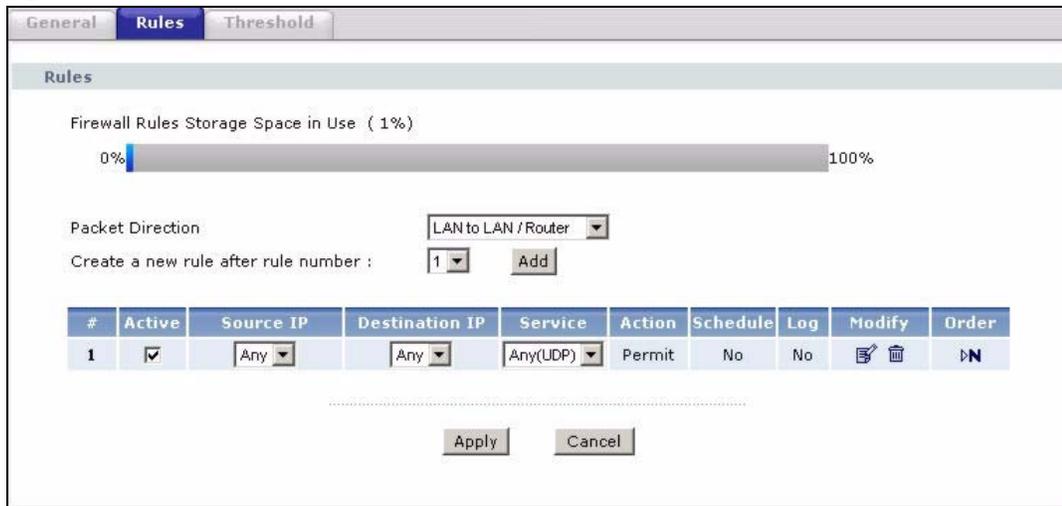
13.6 Firewall Rules Summary

Note: The ordering of your rules is very important as rules are applied in turn.

Refer to [Section 12.1 on page 149](#) for more information.

Click **Security > Firewall > Rules** to bring up the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

Figure 78 Firewall Rules



The following table describes the labels in this screen.

Table 55 Firewall Rules

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyXEL Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click Add to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the General screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any .
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any .
Service	This drop-down list box displays the services to which this firewall rule applies. See Appendix 28 on page 293 for more information.
Action	This field displays whether the firewall silently discards packets (Drop), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (Reject) or allows the passage of packets (Permit).
Schedule	This field tells you whether a schedule is specified (Yes) or not (No).

Table 55 Firewall Rules (continued)

LABEL	DESCRIPTION
Log	This field shows you whether a log is created when packets match this rule (Yes) or not (No).
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Order	Click the Move icon to display the Move the rule to field. Type a number in the Move the rule to field and click the Move button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

13.6.1 Configuring Firewall Rules

Refer to [Section 12.1 on page 149](#) for more information.

In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

Figure 79 Firewall: Edit Rule

Edit Rule 2

Active
 Action for Matched Packets: Permit

Source Address

Address Type: Any Address

Start IP Address: 0.0.0.0 Add >>

End IP Address: 0.0.0.0 Edit <<

Subnet Mask: 0.0.0.0 Delete

Source Address List

Any

Destination Address

Address Type: Any Address

Start IP Address: 0.0.0.0 Add >>

End IP Address: 0.0.0.0 Edit <<

Subnet Mask: 0.0.0.0 Delete

Destination Address List

Any

Service

Available Services

Any(All)
 Any(ICMP)
 AIMNEW-ICQ(TCP:5190)
 AUTH(TCP:113)
 BGP(TCP:179)

Selected Services

Any(UDP)
 Any(TCP)

Add >> Remove

[Edit Customized Services](#)

Schedule

Day to Apply

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Apply : (24-Hour Format)

All day

Start hour minute End hour minute

Log

Log Packet Detail Information.

Alert

Send Alert Message to Administrator When Matched.

Back
 Apply
 Cancel

The following table describes the labels in this screen.

Table 56 Firewall: Edit Rule

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select Drop to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select Reject to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select Permit to allow the passage of the packets.
Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: Single Address , Range Address , Subnet Address and Any Address .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click Add >> to add a new address to the Source or Destination Address box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click Edit << .
Delete	Highlight an existing source or destination address from the Source or Destination Address box above and click Delete to remove it.
Services	
Available/ Selected Services	Please see Appendix 28 on page 293 for more information on services available. Highlight a service from the Available Services box on the left, then click Add >> to add it to the Selected Services box on the right. To remove a service, highlight it in the Selected Services box on the right, then click Remove .
Edit Customized Service	Click the Edit Customized Services link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select All Day or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created or not. Go to the Log Settings page and select the Access Control logs category to have the ZyXEL Device record these logs.
Alert	
Send Alert Message to Administrator When Matched	Select the check box to have the ZyXEL Device generate an alert when the rule is matched.
Back	Click Back to return to the previous screen.

Table 56 Firewall: Edit Rule (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

13.6.2 Customized Services

Configure customized services and port numbers not predefined by the ZyXEL Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix E on page 293](#) for some examples. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Refer to [Section 12.1 on page 149](#) for more information.

Figure 80 Firewall: Customized Services

No.	Name	Protocol	Port
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Back

The following table describes the labels in this screen.

Table 57 Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to the Firewall Customized Services Config screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (TCP , UDP or TCP/UDP) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click Back to return the Firewall Edit Rule screen.

13.6.3 Configuring A Customized Service

Click a rule number in the **Firewall Customized Services** screen to create a new custom port or edit an existing one. This action displays the following screen.

Refer to [Section 12.1 on page 149](#) for more information.

Figure 81 Firewall: Configure Customized Services

The following table describes the labels in this screen.

Table 58 Firewall: Configure Customized Services

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (TCP , UDP or TCP/UDP) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click Single to specify one port only or Range to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to return to the previously saved settings.
Delete	Click Delete to delete the current rule.

13.7 Example Firewall Rule

The following Internet firewall rule example allows a hypothetical “MyService” connection from the Internet.

- 1 Click **Security > Firewall > Rules**.
- 2 Select **WAN to LAN** in the **Packet Direction** field.

Figure 82 Firewall Example: Rules

General **Rules** Threshold

Rules

Firewall Rules Storage Space in Use (3%)

0% 100%

Packet Direction WAN to LAN

Create a new rule after rule number : 0 Add

#	Active	Source IP	Destination IP	Service	Action	Schedule	Log	Modify	Order
.....									

Apply Cancel

- 3** In the **Rules** screen, select the index number after that you want to add the rule. For example, if you select “6”, your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
- 4** Click **Add** to display the firewall rule configuration screen.
- 5** In the **Edit Rule** screen, click the **Edit Customized Services** link to open the **Customized Service** screen.
- 6** Click an index number to display the **Customized Services Config** screen and configure the screen as follows and click **Apply**.

Figure 83 Edit Custom Port Example

Config

Service Name MyService

Service Type TCP/UDP

Port Configuration

Type Single Port Range

Port Number From 123 To 123

Apply Cancel Delete

- 7** Select **Any** in the **Destination Address** box and then click **Delete**.
- 8** Configure the destination address screen as follows and click **Add**.

Figure 84 Firewall Example: Edit Rule: Destination Address

The screenshot shows the 'Edit Rule 1' configuration window. At the top, the rule is active and set to 'Permit'. The 'Source Address' section is currently selected, showing 'Any Address' type and '0.0.0.0' for start and end IP addresses. The 'Destination Address' section is visible below, showing 'Range Address' type with a start IP of '10.0.0.10' and an end IP of '10.0.0.15'. The 'Service' section is partially visible at the bottom.

Edit Rule 1	
<input checked="" type="checkbox"/> Active	Action for Matched Packets: Permit
Source Address	
Address Type: Any Address	Source Address List: Any
Start IP Address: 0.0.0.0	Add >>
End IP Address: 0.0.0.0	Edit <<
Subnet Mask: 0.0.0.0	Delete
Destination Address	
Address Type: Range Address	Destination Address List: 10.0.0.10 - 10.0.0.15
Start IP Address: 10.0.0.10	Add >>
End IP Address: 10.0.0.15	Edit <<
Subnet Mask: 0.0.0.0	Delete
Service	

- 9** Use the **Add >>** and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.

Note: Custom services show up with an "*" before their names in the **Services** list box and the **Rules** list box.

Figure 85 Firewall Example: Edit Rule: Select Customized Services

Edit Rule 2

Active
Action for Matched Packets: **Permit**

Source Address

Address Type: **Any Address**
 Start IP Address: **0.0.0.0**
 End IP Address: **0.0.0.0**
 Subnet Mask: **0.0.0.0**

Source Address List: **Any**

Buttons: Add >>, Edit <<, Delete

Destination Address

Address Type: **Range Address**
 Start IP Address: **10.0.0.10**
 End IP Address: **10.0.0.15**
 Subnet Mask: **0.0.0.0**

Destination Address List: **10.0.0.10 - 10.0.0.15**

Buttons: Add >>, Edit <<, Delete

Service

Available Services: **Any(All), Any(ICMP), AIMNEW-ICQ(TCP:5190), AUTH(TCP:113), BGP(TCP:179)**

Selected Services: ***MyService(TCP/UDP:123)**

Buttons: Add >>, Remove

[Edit Customized Services](#)

Schedule

Day to Apply: Everyday
 Sun Mon Tue Wed Thu Fri Sat

Time of Day to Apply : (24-Hour Format)
 All day
 Start hour minute End hour minute

Log: Log Packet Detail Information.

Alert: Send Alert Message to Administrator When Matched.

Buttons: **Apply**, Cancel

On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.

Rule 1 allows a “MyService” connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

Figure 86 Firewall Example: Rules: MyService

#	Active	Source IP	Destination IP	Service	Action	Schedule	Log	Modify	Order
1	<input checked="" type="checkbox"/>	Any	10.0.0.10 - 10.0.0.15	*MyService(TCP/UDP:123)	Permit	No	No		⤴ ⤵

13.8 DoS Thresholds

For DoS attacks, the ZyXEL Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

Refer to [Section 13.8.3 on page 177](#) to configure thresholds.

13.8.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for most small offices. Factors influencing choices for threshold values are:

- The maximum number of opened sessions.
- The minimum capacity of server backlog in your LAN network.
- The CPU power of servers in your LAN network.
- Network bandwidth.
- Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.

You should make any changes to the threshold values before you continue configuring firewall rules.

13.8.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see [Figure 73 on page 152](#)). For UDP, "half-open" means that the firewall has detected no return traffic.

The ZyXEL Device measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the ZyXEL Device starts deleting half-open sessions as required to accommodate new connection requests. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the ZyXEL Device starts deleting half-open sessions as required to accommodate new connection requests. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

13.8.2.1 TCP Maximum Incomplete and Blocking Time

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the ZyXEL Device starts deleting half-open sessions according to one of the following methods:

- If the **Blocking Time** timeout is 0 (the default), then the ZyXEL Device deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking Time** timeout is greater than 0, then the ZyXEL Device blocks all new connection requests to the host giving the server time to handle the present connections. The ZyXEL Device continues to block all new connection requests until the **Blocking Time** expires.

13.8.3 Configuring Firewall Thresholds

The ZyXEL Device also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall**, and **Threshold** to bring up the next screen.

Figure 87 Firewall: Threshold

The following table describes the labels in this screen.

Table 59 Firewall: Threshold

LABEL	DESCRIPTION	DEFAULT VALUES
Denial of Service Thresholds		
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the ZyXEL Device to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.

Table 59 Firewall: Threshold (continued)

LABEL	DESCRIPTION	DEFAULT VALUES
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set Maximum Incomplete High to lower than the current Maximum Incomplete Low number.	100 existing half-open sessions. The above values causes the ZyXEL Device to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	30 existing half-open TCP sessions.
Action taken when the TCP Maximum Incomplete reached threshold		
Delete the Oldest Half Open Session when New Connection Request Comes.	Select this radio button to clear the oldest half open session when a new connection request comes.	
Deny New Connection Request for	Select this radio button and specify for how long the ZyXEL Device should block new connection requests when TCP Maximum Incomplete is reached. Enter the length of blocking time in minutes (between 1 and 256).	
Apply	Click Apply to save your changes back to the ZyXEL Device.	
Cancel	Click Cancel to begin configuring this screen afresh.	

CHAPTER 14

Content Filtering

This chapter covers how to configure content filtering.

14.1 Content Filtering Overview

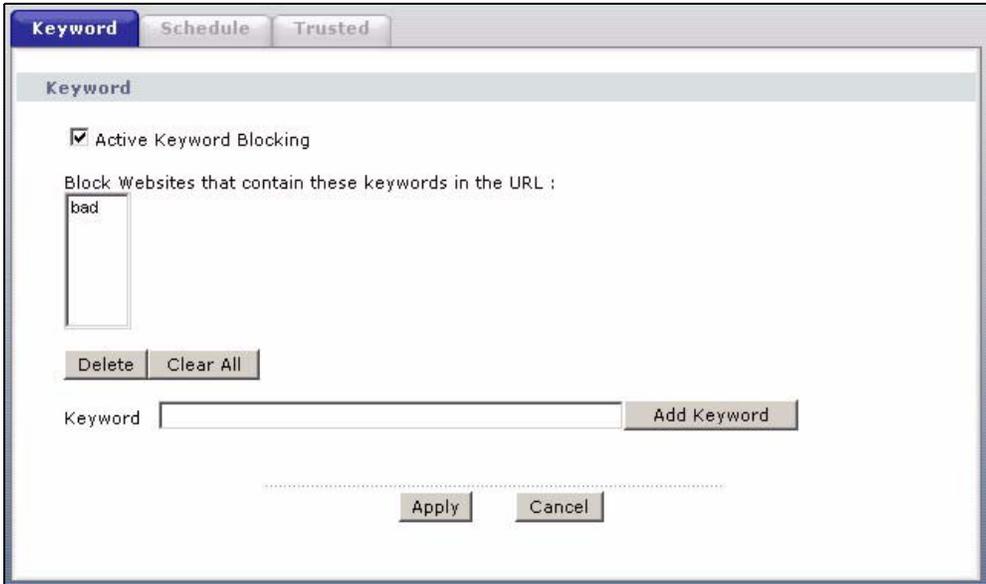
Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering gives you the ability to block web sites that contain key words (that you specify) in the URL. You can set a schedule for when the ZyXEL Device performs content filtering. You can also specify trusted IP addresses on the LAN for which the ZyXEL Device will not perform content filtering.

14.2 Configuring Keyword Blocking

Use this screen to block sites containing certain keywords in the URL. For example, if you enable the keyword "bad", the ZyXEL Device blocks all sites containing this keyword including the URL `http://www.website.com/bad.html`, even if it is not included in the Filter List.

To have your ZyXEL Device block Web sites containing keywords in their URLs, click **Security > Content Filter**. The screen appears as shown.

Figure 88 Content Filter: Keyword



The screenshot shows a web-based configuration interface for the Content Filter: Keyword. The interface has three tabs: "Keyword" (selected), "Schedule", and "Trusted". Under the "Keyword" tab, there is a section titled "Keyword" with a checked checkbox for "Active Keyword Blocking". Below this, a text box labeled "Block Websites that contain these keywords in the URL :" contains the keyword "bad". There are "Delete" and "Clear All" buttons below the text box. At the bottom, there is a "Keyword" input field and an "Add Keyword" button. At the very bottom, there are "Apply" and "Cancel" buttons.

The following table describes the labels in this screen.

Table 60 Content Filter: Keyword

LABEL	DESCRIPTION
Active Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the ZyXEL Device to block.
Delete	Highlight a keyword in the box and click Delete to remove it.
Clear All	Click Clear All to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click Add Keyword 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.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

14.3 Configuring the Schedule

To set the days and times for the ZyXEL Device to perform content filtering, click **Security > Content Filter > Schedule**. The screen appears as shown.

Figure 89 Content Filter: Schedule

Day	Active	Start Time	End Time
Monday	<input checked="" type="checkbox"/>	8 hr 0 min	17 hr 30 min
Tuesday	<input checked="" type="checkbox"/>	0 hr 0 min	0 hr 0 min
Wednesday	<input checked="" type="checkbox"/>	0 hr 0 min	0 hr 0 min
Thursday	<input checked="" type="checkbox"/>	0 hr 0 min	0 hr 0 min
Friday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min
Saturday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min
Sunday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min

The following table describes the labels in this screen.

Table 61 Content Filter: Schedule

LABEL	DESCRIPTION
Schedule	Select Active Everyday to Block to make the content filtering active everyday. Otherwise, select Edit Daily to Block and configure which days of the week (or everyday) and which time of the day you want the content filtering to be active.
Active	Select the check box to have the content filtering to be active on the selected day.
Start Time	Enter the time when you want the content filtering to take effect in hour-minute format.
End Time	Enter the time when you want the content filtering to stop in hour-minute format.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to return to the previously saved settings.

14.4 Configuring Trusted Computers

To exclude a range of users on the LAN from content filtering on your ZyXEL Device, click **Security > Content Filter > Trusted**. The screen appears as shown.

Figure 90 Content Filter: Trusted

The following table describes the labels in this screen.

Table 62 Content Filter: Trusted

LABEL	DESCRIPTION
Trusted User IP Range	
From	Type the IP address of a computer (or the beginning IP address of a specific range of computers) on the LAN that you want to exclude from content filtering.
To	Type the ending IP address of a specific range of users on your LAN that you want to exclude from content filtering. Leave this field blank if you want to exclude an individual computer.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

CHAPTER 15

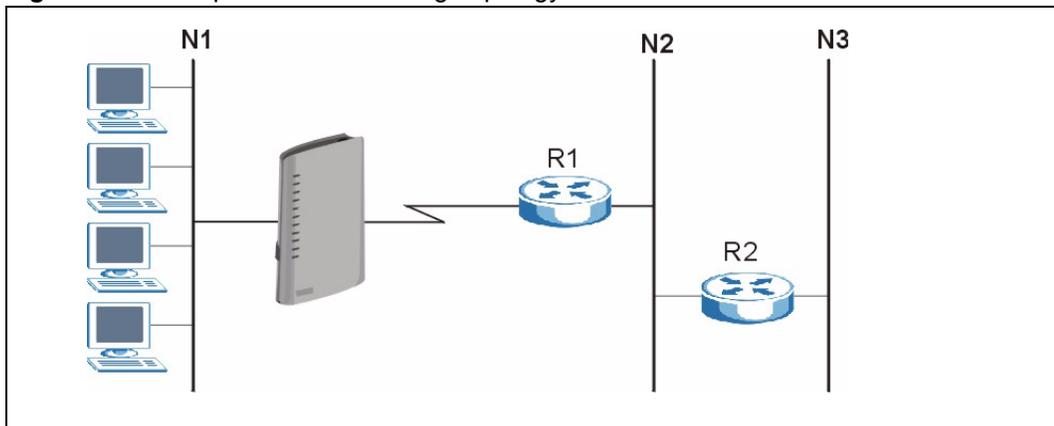
Static Route

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

15.1 Static Route

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 1. 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 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

Figure 91 Example of Static Routing Topology



15.2 Configuring Static Route

Click **Advanced** > **Static Route** to open the **Static Route** screen.

Figure 92 Static Route

#	Active	Name	Destination	Gateway	Modify
1	-	-	-	-	
2	-	-	-	-	
3	-	-	-	-	
4	-	-	-	-	
5	-	-	-	-	
6	-	-	-	-	
7	-	-	-	-	
8	-	-	-	-	
9	-	-	-	-	
10	-	-	-	-	
11	-	-	-	-	
12	-	-	-	-	
13	-	-	-	-	
14	-	-	-	-	
15	-	-	-	-	
16	-	-	-	-	

The following table describes the labels in this screen.

Table 63 Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field shows whether this static route is active (Yes) or not (No).
Name	This is the name that describes or identifies this route.
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 a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the delete icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

15.2.1 Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 93 Static Route Edit

The following table describes the labels in this screen.

Table 64 Static Route Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
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 a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 16

Bandwidth Management

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

16.1 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) must be less than or equal to the WAN speed that you configure in the **Bandwidth Management Summary** screen.
- The sum of the bandwidth allotments that apply to the LAN port (WAN to LAN) must be less than or equal to the LAN speed that you configure in the **Bandwidth Management Summary** screen.

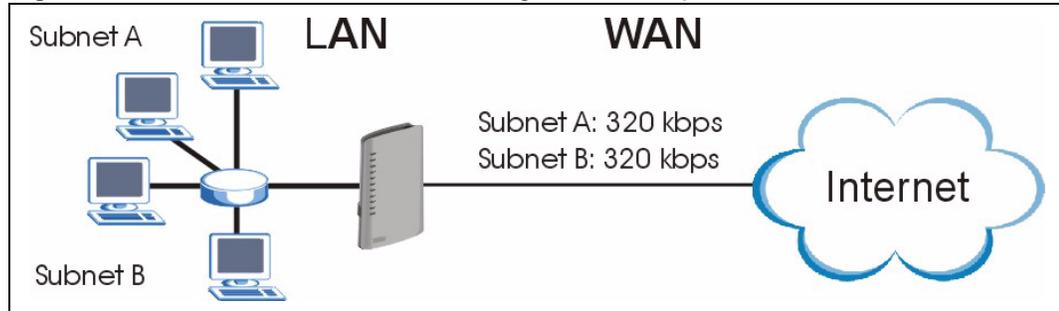
16.2 Application-based Bandwidth Management

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

16.3 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 94 Subnet-based Bandwidth Management Example

16.4 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 65 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	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

16.5 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The ZyXEL Device has two types of scheduler: fairness-based and priority-based.

16.5.1 Priority-based Scheduler

With the priority-based scheduler, the ZyXEL Device forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

16.5.2 Fairness-based Scheduler

The ZyXEL Device divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

16.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see [Figure 95 on page 191](#)) allows the ZyXEL Device to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyXEL Device first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the ZyXEL Device divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the ZyXEL Device gives extra bandwidth to that class.

When multiple classes require more bandwidth, the ZyXEL Device gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The ZyXEL Device distributes the available bandwidth equally among classes with the same priority level.

16.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

Do the following to configure the ZyXEL Device to allow bandwidth for traffic that is not defined in a bandwidth filter.

- 1 Do not enable the interface's **Maximize Bandwidth Usage** option.
- 2 Leave some of the interface's bandwidth unbudgeted. Make sure that the interface's root class has more bandwidth than the sum of the bandwidths of the interface's bandwidth management rules.

16.6.2 Maximize Bandwidth Usage Example

Here is an example of a ZyXEL Device that has maximize bandwidth usage enabled on an interface. The following table shows each bandwidth class's bandwidth budget. The classes are set up based on subnets. The interface is set to 10240 kbps. Each subnet is allocated 2048 kbps. The unbudgeted 2048 kbps allows traffic not defined in any of the bandwidth filters to go out when you do not select the maximize bandwidth option.

Table 66 Maximize Bandwidth Usage Example

BANDWIDTH CLASSES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: 2048 kbps
	Sales: 2048 kbps
	Marketing: 2048 kbps
	Research: 2048 kbps

The ZyXEL Device divides up the unbudgeted 2048 kbps among the classes that require more bandwidth. If the administration department only uses 1024 kbps of the budgeted 2048 kbps, the ZyXEL Device also divides the remaining 1024 kbps among the classes that require more bandwidth. Therefore, the ZyXEL Device divides a total of 3072 kbps of unbudgeted and unused bandwidth among the classes that require more bandwidth.

16.6.2.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the priorities of the bandwidth classes and the amount of bandwidth that each class gets.

Table 67 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

BANDWIDTH CLASSES, PRIORITIES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: Priority 4, 1024 kbps
	Sales: Priority 6, 3584 kbps
	Marketing: Priority 6, 3584 kbps
	Research: Priority 5, 2048 kbps

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The sales and marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1536 kbps or more of extra bandwidth, the ZyXEL Device divides the total 3072 kbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1536 kbps extra to each for a total of 3584 kbps for each) because they both have the highest priority level.
- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

16.6.2.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the amount of bandwidth that each class gets.

Table 68 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

BANDWIDTH CLASSES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: 1024 kbps
	Sales: 3072 kbps
	Marketing: 3072 kbps
	Research: 3072 kbps

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The ZyXEL Device divides the total 3072 kbps total of unbudgeted and unused bandwidth equally among the other classes. 1024 kbps extra goes to each so the other classes each get a total of 3072 kbps.

16.6.3 Bandwidth Management Priorities

Traffic with a higher priority gets through faster while traffic with a lower priority is dropped if the network is congested. The following table describes the priorities that you can apply to traffic that the ZyXEL Device forwards out through an interface.

Table 69 Bandwidth Management Priorities

PRIORITY	DESCRIPTION
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.

16.7 Configuring Summary

Click **Advanced > Bandwidth MGMT** to open the screen as shown next.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

Figure 95 Bandwidth Management: Summary

Interface	Active	Speed(kbps)	Scheduler	Max Bandwidth Usage
LAN	<input checked="" type="checkbox"/>	100000	Priority-Based	<input checked="" type="checkbox"/> Yes
WAN	<input checked="" type="checkbox"/>	800	Priority-Based	<input checked="" type="checkbox"/> Yes

The following table describes the labels in this screen.

Table 70 Media Bandwidth Management: Summary

LABEL	DESCRIPTION
Interface	<p>These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.</p> <p>Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management.</p>
Active	<p>Select an interface's check box to enable bandwidth management on that interface.</p>
Speed (kbps)	<p>Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.</p> <p>This appears as the bandwidth budget of the interface's root class. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 1000 kbps if your Internet connection has an upstream transmission speed of 1 Mbps.</p> <p>If this number is higher than the interface's actual transmission speed, and you configure bandwidth rules for all of the bandwidth, higher priority traffic could use all of the bandwidth so lower priority traffic does not get through.</p> <p>Note: Unless you enable Max Bandwidth Usage, the ZyXEL Device only uses up to the amount of bandwidth that you configure here. The ZyXEL Device does not use any more bandwidth for the interface's connections, even if the interface has more outgoing bandwidth.</p>
Scheduler	<p>Select either Priority-Based or Fairness-Based from the drop-down menu to control the traffic flow.</p> <p>Select Priority-Based to give preference to bandwidth classes with higher priorities. Select Fairness-Based to treat all bandwidth classes equally.</p>
Max Bandwidth Usage	<p>Select this check box to have the ZyXEL Device divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the transmission speed of this interface (see the Speed field description).</p>
Apply	<p>Click Apply to save your settings back to the ZyXEL Device.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

16.8 Bandwidth Management Rule Setup

You must use the **Bandwidth Management Summary** screen to enable bandwidth management on an interface before you can configure rules for that interface.

Click **Advanced > Bandwidth MGMT > Rule Setup** to open the following screen.

Figure 96 Bandwidth Management: Rule Setup

Summary **Rule Setup** Monitor

Rule Setup

Direction: LAN Service: WWW Priority: High Bandwidth: 10 (kbps) Add

To LAN Interface

#	Rule Name	Destination Port	Priority	Bandwidth(kbps)	Modify
1	WWW	0	High	1000	

Apply Cancel

The following table describes the labels in this screen.

Table 71 Bandwidth Management: Rule Setup

LABEL	DESCRIPTION
Direction	Select LAN to apply bandwidth management to traffic that the ZyXEL Device forwards to the LAN. Select WAN to apply bandwidth management to traffic that the ZyXEL Device forwards to the WAN.
Service	Select a service for your rule or you can select User define to go to the screen where you can define your own.
Priority	Select a priority from the drop down list box. Choose High, Mid or Low .
Bandwidth (kbps)	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule. If you want to leave some bandwidth for traffic that does not match a bandwidth filter, make sure that the interface's root class has more bandwidth than the sum of the bandwidths of the interface's bandwidth management rules.
Add	Click this button to save your rule. It displays in the following table.
#	This is the number of an individual bandwidth management rule.
Active	This displays whether the rule is enabled. Select this check box to have the ZyXEL Device apply this bandwidth management rule. Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule. Enabling a bandwidth management rule also allows you to control the maximum amounts of bandwidth that can be used by traffic that matches the rule.
Rule Name	This is the name of the rule.
Destination Port	This is the port number of the destination. 0 means any destination port.
Priority	This is the priority of this rule.
Bandwidth (kbps)	This is the maximum bandwidth allowed for the rule in kbps.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing rule.

Table 71 Bandwidth Management: Rule Setup (continued)

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

16.8.1 Rule Configuration

Click the **Edit** icon or **User define** in the **Service** field to configure a bandwidth management rule. Use bandwidth rules to allocate specific amounts of bandwidth capacity (bandwidth budgets) to specific applications and/or subnets.

Figure 97 Bandwidth Management Rule Configuration

See [Appendix E on page 293](#) for a list of commonly-used services. The following table describes the labels in this screen.

Table 72 Bandwidth Management Rule Configuration

LABEL	DESCRIPTION
Rule Configuration	
Active	Select this check box to have the ZyXEL Device apply this bandwidth management rule. Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule. Enabling a bandwidth management rule also allows you to control the maximum amounts of bandwidth that can be used by traffic that matches the rule.
Rule Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.

Table 72 Bandwidth Management Rule Configuration (continued)

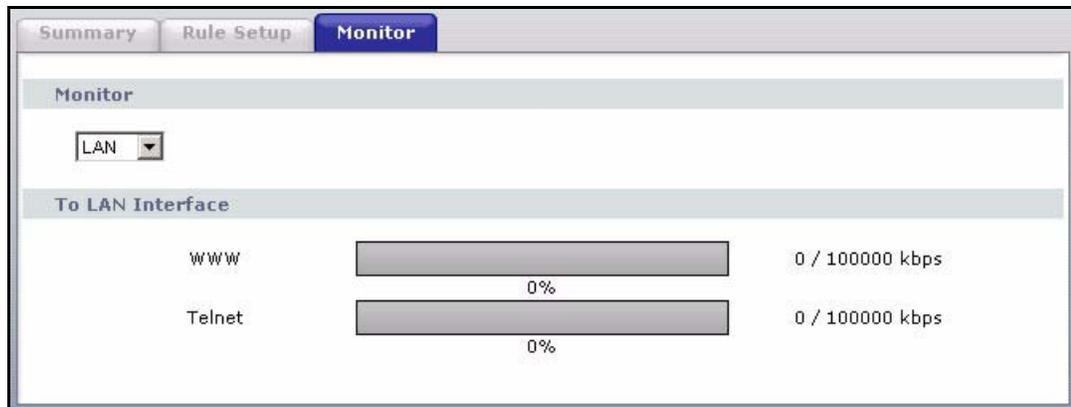
LABEL	DESCRIPTION
BW Budget	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule.
Priority	Select a priority from the drop down list box. Choose High , Mid or Low .
Use All Managed Bandwidth	Select this option to allow a rule to borrow unused bandwidth on the interface. Bandwidth borrowing is governed by the priority of the rules. That is, a rule with the highest priority is the first to borrow bandwidth. Do not select this if you want to leave bandwidth available for other traffic types or if you want to restrict the amount of bandwidth that can be used for the traffic that matches this rule.
Filter Configuration	
Service	<p>This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).</p> <p>SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select SIP from the drop-down list box to configure this bandwidth filter for traffic that uses SIP.</p> <p>File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select FTP from the drop-down list box to configure this bandwidth filter for FTP traffic.</p> <p>H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Select H.323 from the drop-down list box to configure this bandwidth filter for traffic that uses H.323.</p> <p>Select User defined from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select User defined, you need to configure at least one of the following fields (other than the Subnet Mask fields which you only enter if you also enter a corresponding destination or source IP address).</p>
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 appendix for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See Appendix E on page 293 for some common services and port numbers. A blank destination IP address means any destination IP address.
Source Address	Enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Source Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a Source Address . Refer to the appendix for more information on IP subnetting. A blank source port means any source port number.
Source Port	Enter the port number of the source. See Appendix E on page 293 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. 0 means any protocol number.
Back	Click Back to go to the previous screen.

Table 72 Bandwidth Management Rule Configuration (continued)

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

16.9 Bandwidth Monitor

To view the ZyXEL Device's bandwidth usage and allotments, click **Advanced > Bandwidth MGMT > Monitor**. The screen appears as shown. Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth rules.

Figure 98 Bandwidth Management: Monitor

CHAPTER 17

Dynamic DNS Setup

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

17.1 Dynamic DNS Overview

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.

17.1.1 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.

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

See [Section 17.2 on page 197](#) for configuration instruction.

17.2 Configuring Dynamic DNS

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

See [Section 17.1 on page 197](#) for more information.

Figure 99 Dynamic DNS

The following table describes the fields in this screen.

Table 73 Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is 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	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type 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.

Table 73 Dynamic DNS (continued)

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP Address	Select this option only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
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.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 18

Remote Management Configuration

This chapter provides information on configuring remote management.

18.1 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.

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 **LAN** only, **WAN** only 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 **Access Status** 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

18.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- You have disabled that service in one of the remote management screens.

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

18.1.2 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.

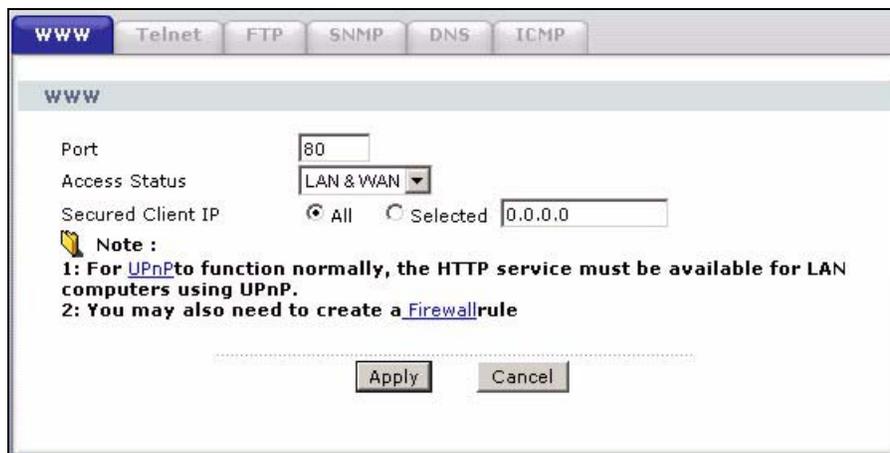
18.1.3 System Timeout

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.

18.2 WWW

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

Figure 100 Remote Management: WWW



The screenshot shows the 'WWW' configuration page in a web browser. At the top, there are tabs for 'WWW', 'Telnet', 'FTP', 'SNMP', 'DNS', and 'ICMP'. The 'WWW' tab is selected. Below the tabs, the page title is 'www'. The configuration fields are:

- Port: 80
- Access Status: LAN & WAN (dropdown menu)
- Secured Client IP: All Selected

Below the fields is a **Note** section with a yellow icon:

Note :
1: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
2: You may also need to create a Firewall rule

At the bottom of the page are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

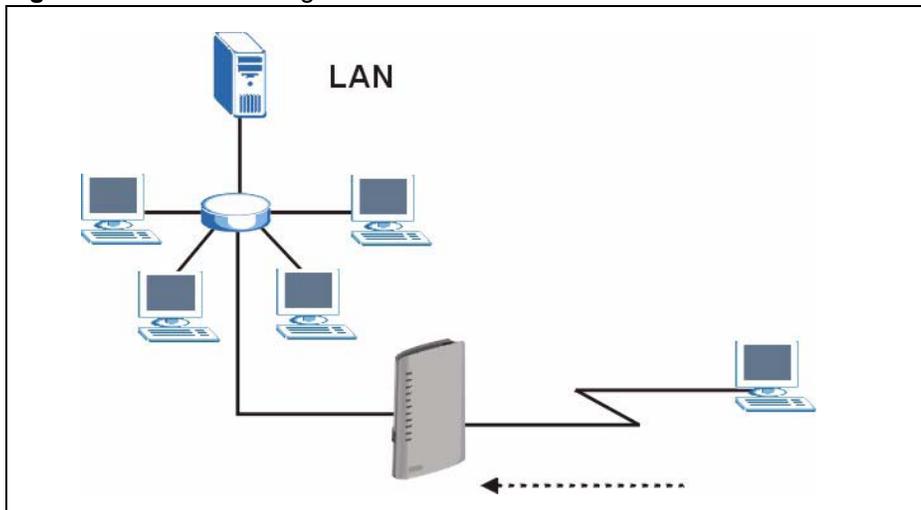
Table 74 Remote Management: WWW

LABEL	DESCRIPTION
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.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	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 settings back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

18.3 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.

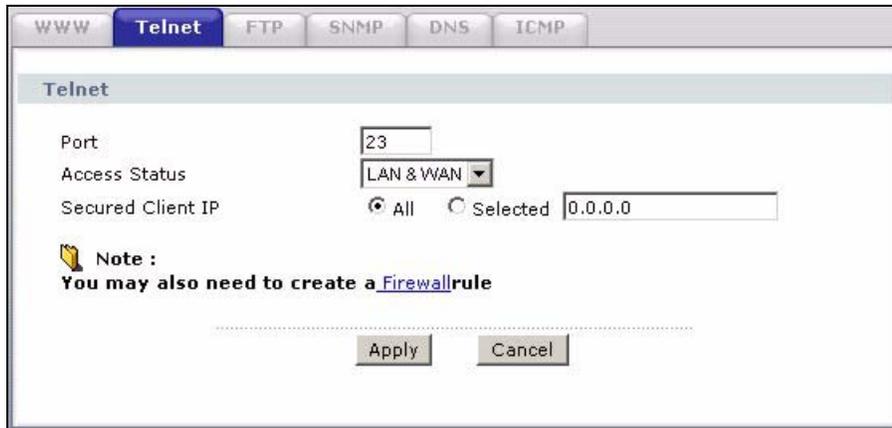
Figure 101 Telnet Configuration on a TCP/IP Network



18.4 Configuring Telnet

Click **Advanced > Remote MGMT > Telnet** tab to display the screen as shown.

Figure 102 Remote Management: Telnet



The following table describes the labels in this screen.

Table 75 Remote Management: Telnet

LABEL	DESCRIPTION
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.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	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.
Cancel	Click Cancel to begin configuring this screen afresh.

18.5 Configuring FTP

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

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

Figure 103 Remote Management: FTP

The following table describes the labels in this screen.

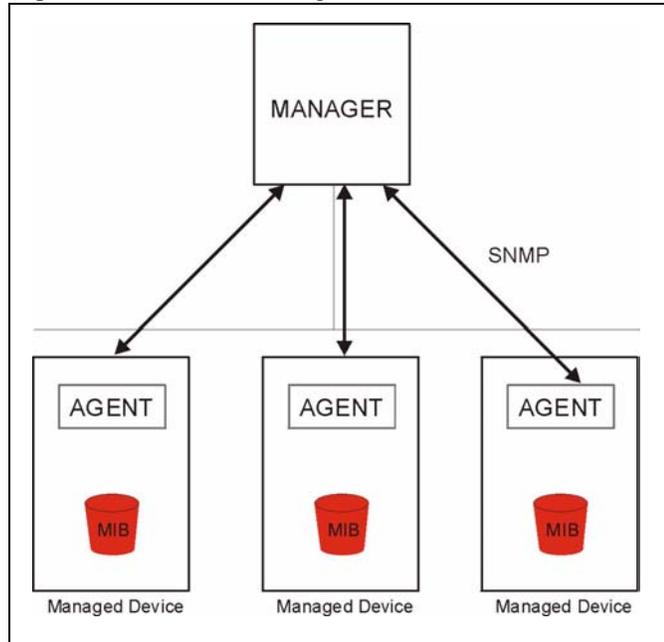
Table 76 Remote Management: FTP

LABEL	DESCRIPTION
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.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	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.
Cancel	Click Cancel to begin configuring this screen afresh.

18.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

Figure 104 SNMP Management Model

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

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

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

18.6.1 Supported MIBs

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

18.6.2 SNMP Traps

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

Table 77 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CLI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

18.6.3 Configuring SNMP

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

Figure 105 Remote Management: SNMP

The following table describes the labels in this screen.

Table 78 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP	
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.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	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.
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

18.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to [Chapter 8 on page 95](#) for background information.

To change your ZyXEL Device's DNS settings, click **Advanced > Remote MGMT > DNS**. The screen appears as shown. Use this screen to set from which IP address the ZyXEL Device will accept DNS queries and on which interface it can send them your ZyXEL Device's DNS settings.

Figure 106 Remote Management: DNS

The following table describes the labels in this screen.

Table 79 Remote Management: DNS

LABEL	DESCRIPTION
Port	The DNS service port number is 53 and cannot be changed here.
Access Status	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP	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.
Cancel	Click Cancel to begin configuring this screen afresh.

18.8 Configuring ICMP

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

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. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

Note: If you want your device to respond to pings and requests for unauthorized services, you may also need to configure the firewall anti probing settings to match.

Figure 107 Remote Management: ICMP



The following table describes the labels in this screen.

Table 80 Remote Management: ICMP

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.
Do not respond to requests for unauthorized services	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. 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.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 19

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

19.1 Introducing Universal Plug and Play

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

See [Section 19.2.1 on page 212](#) for configuration instructions.

19.1.1 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.

19.1.2 NAT Traversal

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

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

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

See [Chapter 9 on page 109](#) for more information on NAT.

19.1.3 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.

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

19.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

UPnP broadcasts are only allowed on the LAN.

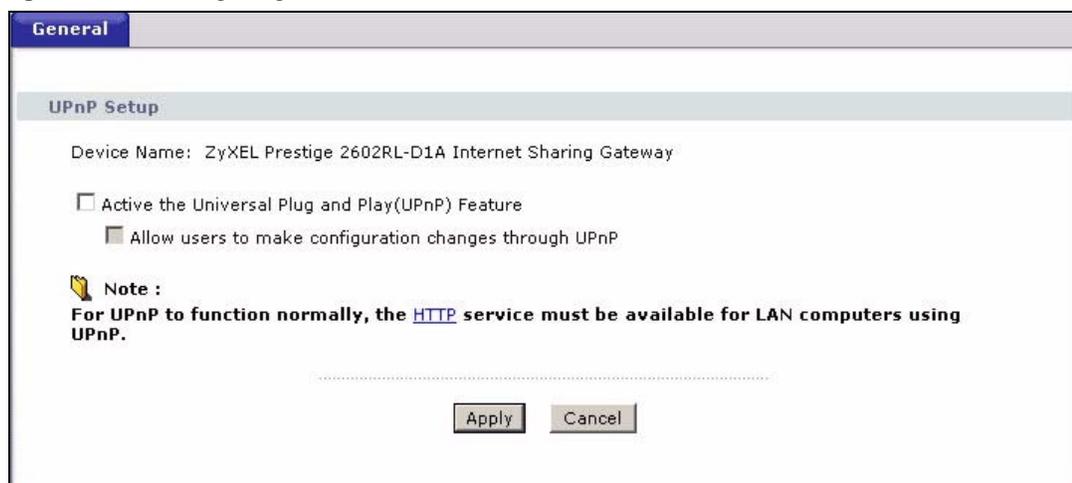
See later sections for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

19.2.1 Configuring UPnP

Click **Advanced > UPnP** to display the screen shown next.

See [Section 19.1 on page 211](#) for more information.

Figure 108 Configuring UPnP



The following table describes the fields in this screen.

Table 81 Configuring UPnP

LABEL	DESCRIPTION
Active the Universal Plug and Play (UPnP) Feature	Select this check box 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	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click Apply to save the setting to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

19.3 Installing UPnP in Windows Example

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

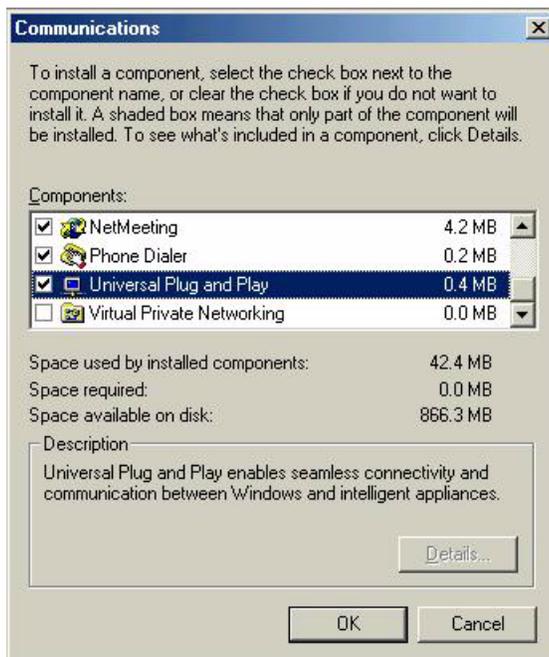
Installing UPnP in Windows Me

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

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

Figure 109 Add/Remove Programs: Windows Setup: Communication

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

Figure 110 Add/Remove Programs: Windows Setup: Communication: Components

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

Installing UPnP in Windows XP

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

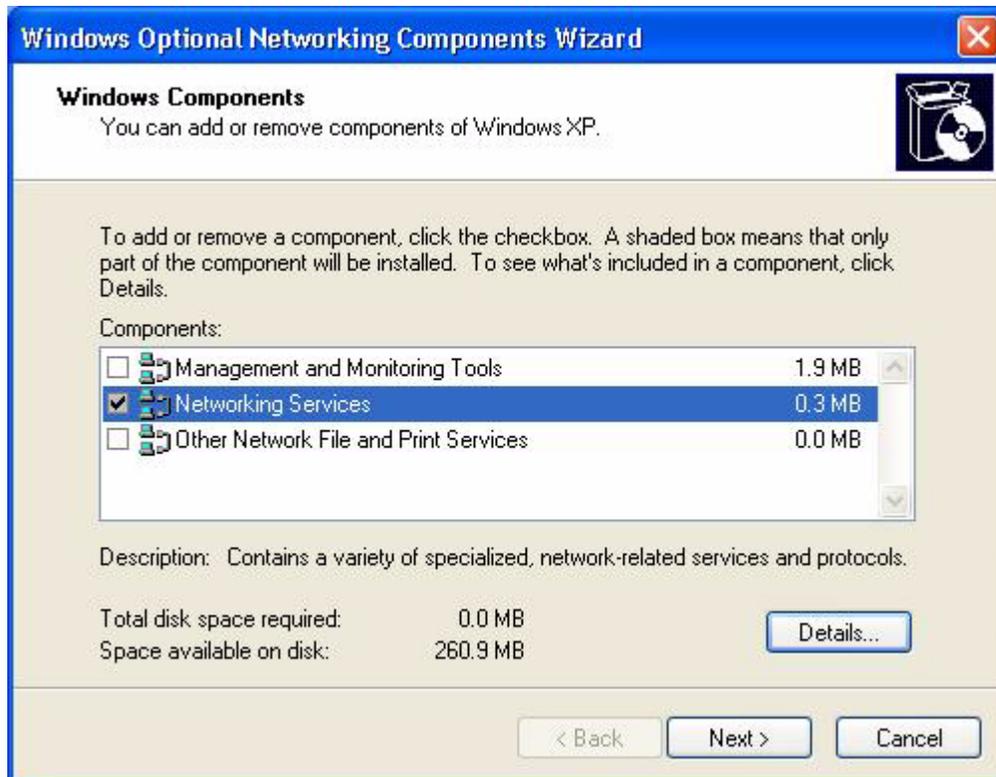
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components**

Figure 111 Network Connections



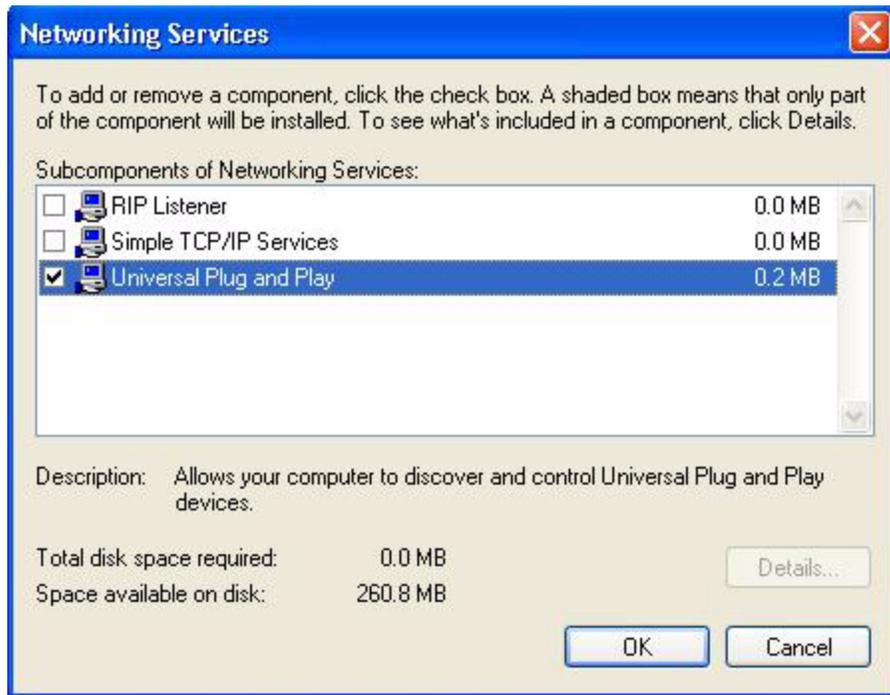
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 112 Windows Optional Networking Components Wizard



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

Figure 113 Networking Services



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

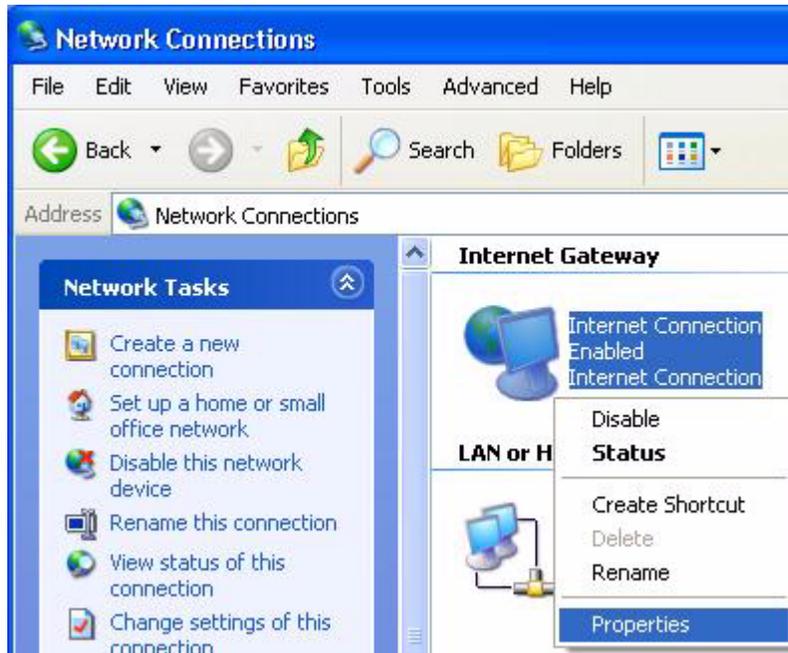
19.4 Using UPnP in Windows XP Example

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

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

Auto-discover Your UPnP-enabled Network Device

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

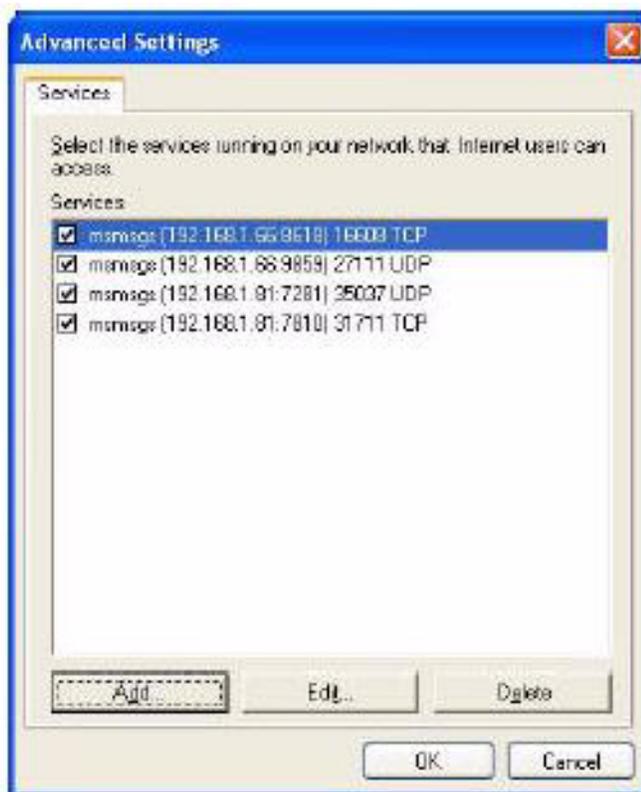
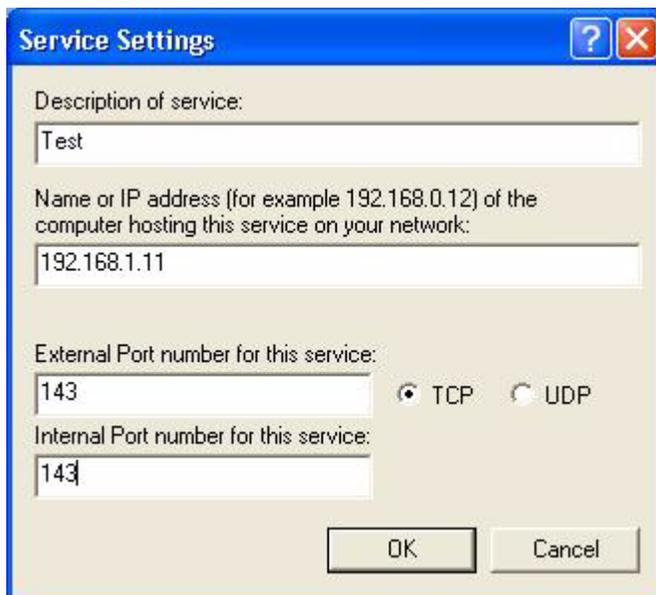
Figure 114 Network Connections

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

Figure 115 Internet Connection Properties



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

Figure 116 Internet Connection Properties: Advanced Settings**Figure 117** Internet Connection Properties: Advanced Settings: Add

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

Figure 118 System Tray Icon

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

Figure 119 Internet Connection Status

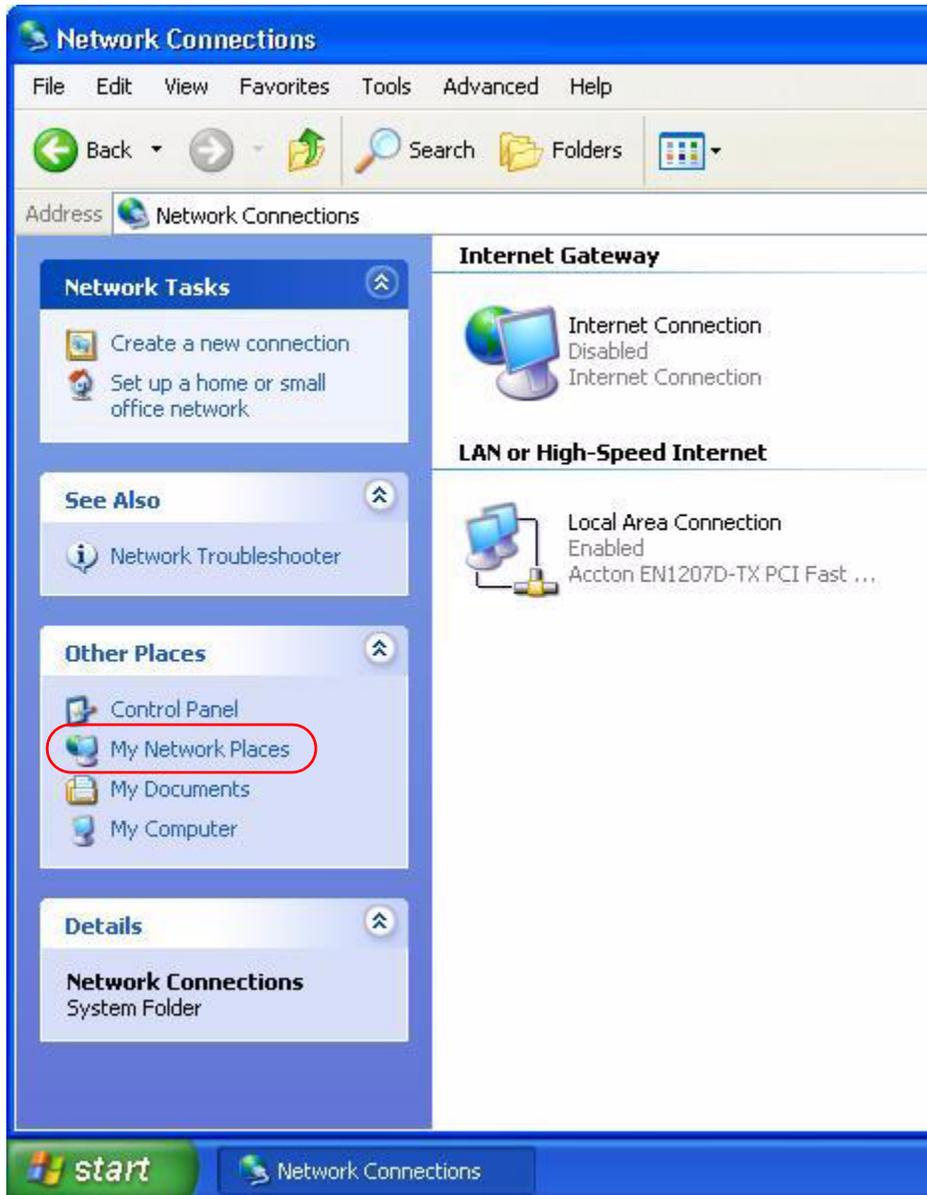
Web Configurator Easy Access

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

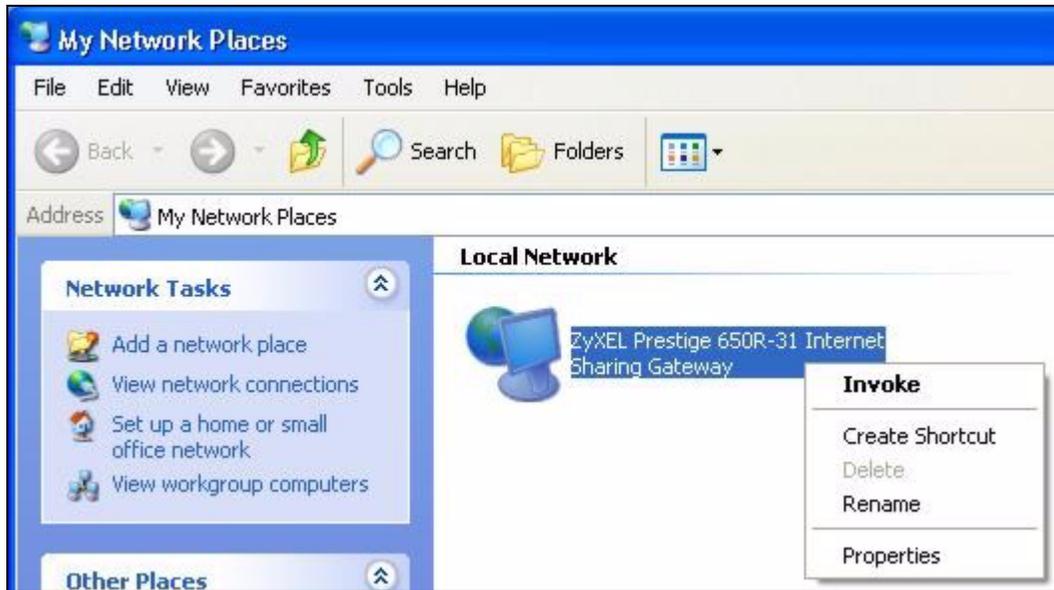
Follow the steps below to access the web configurator.

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

Figure 120 Network Connections



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

Figure 121 Network Connections: My Network Places

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

Figure 122 Network Connections: My Network Places: Properties: Example

CHAPTER 20

System

Use this screen to configure the ZyXEL Device's time and date settings.

20.1 General Setup and System Name

General Setup contains administrative and system-related information. **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, 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**.

20.1.1 General Setup

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), the domain name can be assigned from the ZyXEL Device via DHCP.

Click **Maintenance > System** to open the **General** screen.

Figure 123 System General Setup

The following table describes the labels in this screen.

Table 82 System General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. 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 (either via the web configurator or telnet) 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	
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 a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

20.2 Time Setting

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 124 System Time Setting

The following table describes the fields in this screen.

Table 83 System 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.

Table 83 System Time Setting (continued)

LABEL	DESCRIPTION
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 .
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.
Time Protocol	Select the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, NTP (RFC 1305) , is similar to Time (RFC 868).
Time Server Address	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 Saving	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 Enable Daylight Saving . 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).

Table 83 System Time Setting (continued)

LABEL	DESCRIPTION
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Enable Daylight Saving. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>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.</p> <p>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).</p>
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 21

Logs

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

21.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

21.1.1 Alerts and Logs

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. 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.

21.2 Viewing the Logs

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 21.3 on page 230](#)).

Log entries in red indicate alerts. 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 125 View Log

#	Time	Message	Source	Destination	Notes
1	01/01/2000 00:33:40	WEB Login Successfully			User:admin
2	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1197	ACCESS PERMITTED
3	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1196	ACCESS PERMITTED
4	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1195	ACCESS PERMITTED
5	01/01/2000 00:30:23	WEB Login Successfully			User:user

The following table describes the fields in this screen.

Table 84 View Log

LABEL	DESCRIPTION
Display	The categories that you select in the Log Settings screen 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.
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 E-mail Log Settings fields in Log Settings).
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

21.3 Configuring Log Settings

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 is to record. See [Section 21.1 on page 229](#) for more information.

To change your ZyXEL Device's log settings, click **Maintenance > Logs > Log Settings**. The screen appears as shown.

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

Figure 126 Log Settings

The screenshot shows the 'Log Settings' configuration page. It has a navigation bar with 'View Log' and 'Log Settings' tabs. The main content is organized into three sections:

- E-mail Log Settings:** Contains input fields for 'Mail Server', 'Mail Subject', 'Send Log to', and 'Send Alerts to'. There are checkboxes for 'Enable SMTP Authentication', 'Clear log after sending mail', and a 'Log Schedule' section with dropdowns for 'When Log is Full' (set to 'When Log is Full') and 'Day for Sending Log' (set to 'Monday'). There are also input fields for 'User Name' and 'Password'.
- Syslog Logging:** Includes an 'Active' checkbox, a 'Syslog IP Address' field (set to '0.0.0.0'), and a 'Log Facility' dropdown (set to 'Local 1').
- Active Log and Alert:** Divided into two columns. The left column, 'Log', lists categories like System Maintenance, System Errors, Access Control, UPnP, Forward Web Sites, Blocked Web Sites, Attacks, Any IP, SIP, RTP, and FSM. The right column, 'Send Immediate Alert', lists System Errors, Access Control, Blocked Web Sites, and Attacks. All are currently unchecked.

At the bottom center, there are 'Apply' and 'Cancel' buttons.

The following table describes the fields in this screen.

Table 85 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.

Table 85 Log Settings

LABEL	DESCRIPTION
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. Not all ZyXEL Device models have this field.
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.
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.
Enable 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	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <p>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.</p>
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 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.
Active Log and Alert	
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 customized settings and exit this screen.
Cancel	Click Cancel to return to the previously saved settings.

21.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error message appears.

“SMTP action request failed. ret= ??”. The “??” are described in the following table.

Table 86 SMTP Error Messages

-1 means ZyXEL Device out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

21.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "End of Log" message shows that a complete log has been sent.

Figure 127 E-mail Log Example

```
Subject:
  Firewall Alert From
Date:
  Fri, 07 Apr 2000 10:05:42
From:
  user@zyxel.com
To:
  user@zyxel.com
1|Apr 7 00 |From:192.168.1.1      To:192.168.1.255  |default policy |forward
  | 09:54:03 |UDP      src port:00520 dest port:00520  |<1,00>         |
2|Apr 7 00 |From:192.168.1.131   To:192.168.1.255  |default policy |forward
  | 09:54:17 |UDP      src port:00520 dest port:00520  |<1,00>         |
3|Apr 7 00 |From:192.168.1.6     To:10.10.10.10    |match          |forward
  | 09:54:19 |UDP      src port:03516 dest port:00053  |<1,01>         |
.....{snip}.....
.....{snip}.....
126|Apr 7 00 |From:192.168.1.1     To:192.168.1.255  |match          |forward
  | 10:05:00 |UDP      src port:00520 dest port:00520  |<1,02>         |
127|Apr 7 00 |From:192.168.1.131   To:192.168.1.255  |match          |forward
  | 10:05:17 |UDP      src port:00520 dest port:00520  |<1,02>         |
128|Apr 7 00 |From:192.168.1.1     To:192.168.1.255  |match          |forward
  | 10:05:30 |UDP      src port:00520 dest port:00520  |<1,02>         |
End of Firewall Log
```

CHAPTER 22

Tools

This chapter explains how to upload new firmware, manage configuration files and restart your ZyXEL Device.

Note: Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyXEL Device.

22.1 Introduction

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

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

22.2 Filename Conventions

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

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

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

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

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

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

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

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

Table 87 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyXEL Device.	*.bin

22.3 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

- 1 The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
- 2 You have disabled Telnet service in menu 24.11.
- 3 You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- 4 The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the device will disconnect the Telnet session immediately.

22.4 Firmware Upgrade Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See [Section 22.9 on page 245](#) for upgrading firmware using FTP/TFTP commands.

Figure 128 Firmware Upgrade

The following table describes the labels in this screen.

Table 88 Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
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 Progress** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 129 Firmware Upload In Progress

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 130 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 131 Error Message



22.5 Backup and Restore

See [Section 22.7 on page 241](#) and [Section 22.8 on page 244](#) 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 132 Configuration

The screenshot shows the Configuration page with the following content:

- Backup Configuration:** Click **Backup** to save the current configuration to your computer.
- Restore Configuration:** To restore a previously saved configuration file on your computer to the Prestige, please type a location for storing the configuration file or click **Browse** to look for one, and then click **Upload**.
File Path:
- Reset to Factory Default Settings:** Click **Reset** to clear all user-entered configuration and return the Prestige to the factory default settings.
The following default settings would become effective after click **Reset**
Password :1234
Lan IP : 192.168.1.1
DHCP : Server ,

22.5.1 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.

22.5.2 Restore Configuration

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

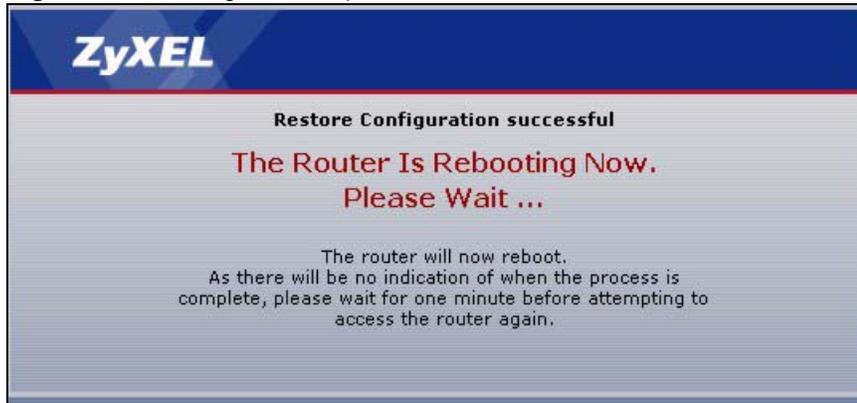
Table 89 Restore Configuration

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

Figure 133 Configuration Upload 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 134 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See [Appendix C on page 273](#) for details on how to set up your computer's IP address.

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

22.5.3 Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

Figure 135 Reset Warning Message



Figure 136 Reset In Process Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to [Section 2.1.2 on page 47](#) for more information on the **RESET** button.

22.6 Restart

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 137 Restart Screen

22.7 Using FTP or TFTP to Back Up Configuration

This section covers how to use FTP or TFTP to save your device's configuration file to your computer.

22.7.1 Using the FTP Commands to Back Up Configuration

- 1 Launch the FTP client on your computer.
- 2 Enter "open", followed by a space and the IP address of your ZyXEL Device.

- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “get” to transfer files from the ZyXEL Device to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

22.7.2 FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device's configuration onto your computer.

Figure 138 FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

22.7.3 Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 90 General Commands for GUI-based FTP Clients

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

22.7.4 Backup Configuration Using TFTP

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

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

- 1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Enter command “`sys stdio 0`” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command “`sys stdio 5`” to restore the five-minute management idle timeout (default) when the file transfer is complete.
- 3 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
- 4 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is “`rom-0`” (rom-zero, not capital o).

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “`get`” to transfer from the ZyXEL Device to the computer and “`binary`” to set binary transfer mode.

22.7.5 TFTP Command Configuration Backup Example

The following is an example TFTP command:

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

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

22.7.6 Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 91 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.1 is the ZyXEL Device's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyXEL Device and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to [Section 22.3 on page 236](#) to read about configurations that disallow TFTP and FTP over WAN.

22.8 Using FTP or TFTP to Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Note: WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR device. When the Restore Configuration process is complete, the device will automatically restart.

22.8.1 Restore Using FTP Session Example

Figure 139 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to [Section 22.3 on page 236](#) to read about configurations that disallow TFTP and FTP over WAN.

22.9 FTP and TFTP Firmware and Configuration File Uploads

This section shows you how to upload firmware and configuration files.

Note: WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

22.9.1 FTP File Upload Command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your device.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

22.9.2 FTP Session Example of Firmware File Upload

Figure 140 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to [Section 22.3 on page 236](#) to read about configurations that disallow TFTP and FTP over WAN.

22.9.3 TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

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

- 1** Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2** Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
- 3** Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
- 4** Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

22.9.4 TFTP Upload Command Example

The following is an example TFTP command:

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

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

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

CHAPTER 23

Diagnostic

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

23.1 General Diagnostic

Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 141 Diagnostic: General

The screenshot shows a web interface for diagnostic tools. At the top, there are two tabs: 'General' and 'DSL Line'. The 'General' tab is active. Below the tabs, there is a section titled 'General'. Inside this section, there is a large text area with the text '- Info -'. At the bottom of the screen, there is a 'TCP/IP Address' input field and a 'Ping' button.

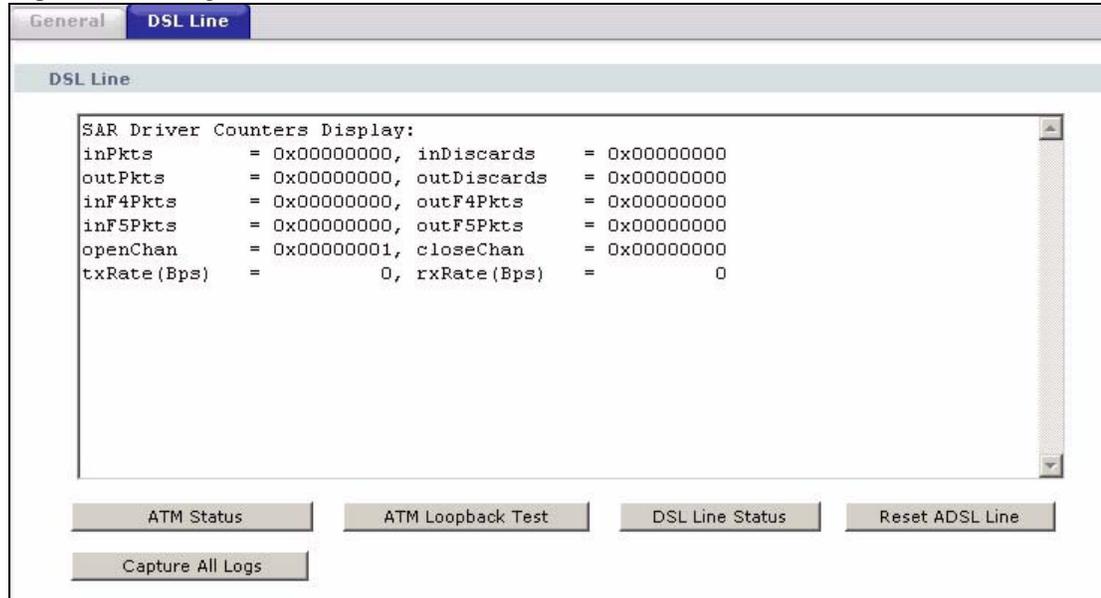
The following table describes the fields in this screen.

Table 92 Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.

23.2 DSL Line Diagnostic

Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

Figure 142 Diagnostic: DSL Line

The following table describes the fields in this screen.

Table 93 Diagnostic: DSL Line

LABEL	DESCRIPTION
ATM Status	<p>Click this button to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed.</p> <p>The SAR driver is</p> <p>These counters are set back to zero whenever the device</p> <p>inPkts is the number of good ATM cells that have been received.</p> <p>inDiscards is the number of received ATM cells that were rejected.</p> <p>outPkts is the number of ATM cells that have been sent.</p> <p>outDiscards is the number of ATM cells sent that were rejected.</p> <p>inF4Pkts is the number of ATM Operations, Administration, and Management (OAM) F4 cells that have been received. See ITU recommendation I.610 for more on OAM for ATM.</p> <p>outF4Pkts is the number of ATM OAM F4 cells that have been sent.</p> <p>inF5Pkts is the number of ATM OAM F5 cells that have been received.</p> <p>outF5Pkts is the number of ATM OAM F5 cells that have been sent.</p> <p>openChan is the number of times that the ZyXEL Device has opened a logical DSL channel.</p> <p>closeChan is the number of times that the ZyXEL Device has closed a logical DSL channel.</p> <p>txRate is the number of bytes transmitted per second.</p> <p>rxRate is the number of bytes received per second.</p>
ATM Loopback Test	<p>Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCI before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.</p>

Table 93 Diagnostic: DSL Line (continued)

LABEL	DESCRIPTION
DSL Line Status	<p>Click this button to view statistics about the DSL connections.</p> <p>noise margin downstream is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is.</p> <p>output power upstream is the amount of power (in decibels) that the ZyXEL Device is using to transmit to the ISP.</p> <p>attenuation downstream is the reduction in amplitude (in decibels) of the DSL signal coming into the ZyXEL Device from the ISP.</p> <p>Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT.</p> <p>The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.</p>
Reset ADSL Line	<p>Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:</p> <pre> "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!" </pre>
Capture All Logs	Click this button to display all logs generated by the DSL line.

CHAPTER 24

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

24.1 Problems Starting Up the ZyXEL Device

Table 94 Troubleshooting Starting Up Your Device

PROBLEM	CORRECTIVE ACTION
None of the lights 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>

24.2 Problems with the LAN

Table 95 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The ETHERNET lights do not turn on.	Check your Ethernet cable connections (refer to the <i>Quick Start Guide</i> for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet Card is working properly.
I cannot access the ZyXEL Device from the LAN.	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.

24.3 Problems with the WAN

Table 96 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The DSL light is off.	Check the telephone wire and connections between the ZyXEL Device DSL port and the wall jack.
	Make sure that the telephone company has checked your phone line and set it up for DSL service.
	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to Section 23.2 on page 249 .
I cannot get a WAN IP address from the ISP. (The INTERNET light is red.)	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name. 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 Section 7.5 on page 86 .
I cannot access the Internet.	Make sure the ZyXEL Device is turned on and connected to the network. Verify your WAN settings. Refer to Chapter 7 on page 81 . 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 PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to Section 7.5 on page 86 . Contact your ISP.

24.4 Problems Accessing the ZyXEL Device

Table 97 Troubleshooting Accessing Your Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	<p>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.</p> <p>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.</p>
I cannot access the web configurator.	<p>Make sure that there is not a telnet session running.</p> <p>Use the ZyXEL Device's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection.</p> <p>Use the ZyXEL Device's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection.</p> <p>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 Chapter 18 on page 201 for details.</p> <p>Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p>
I cannot remotely manage the ZyXEL Device from the LAN or WAN.	<p>You may also need to clear your Internet browser's cache.</p> <p>In Internet Explorer, click Tools and then Internet Options to open the Internet Options screen.</p> <p>In the General tab, click Delete Files. In the pop-up window, select the Delete all offline content check box and click OK. Click OK in the Internet Options screen to close it.</p> <p>If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).</p> <p>In Windows, use arp -d at the command prompt to delete all entries in your computer's ARP table.</p>
	<p>Refer to Chapter 18 on page 201 for scenarios when remote management may not be possible.</p> <p>Use the ZyXEL Device's WAN IP address when configuring from the WAN.</p> <p>Use the ZyXEL Device's LAN IP address when configuring from the LAN.</p>

24.4.1 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.

24.4.1.1 Internet Explorer Pop-up Blockers

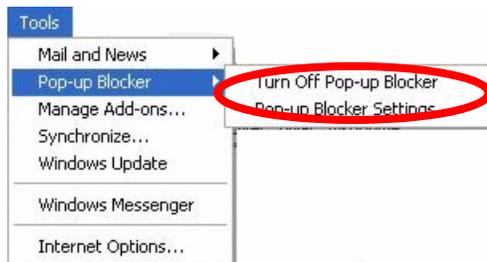
You may have to disable pop-up blocking to log into your device.

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.

24.4.1.1.1 Disable pop-up Blockers

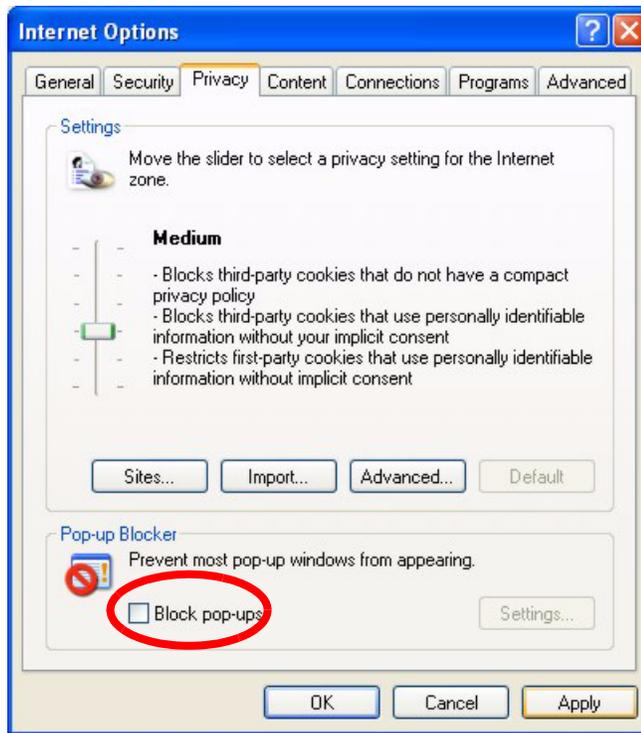
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 143 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.

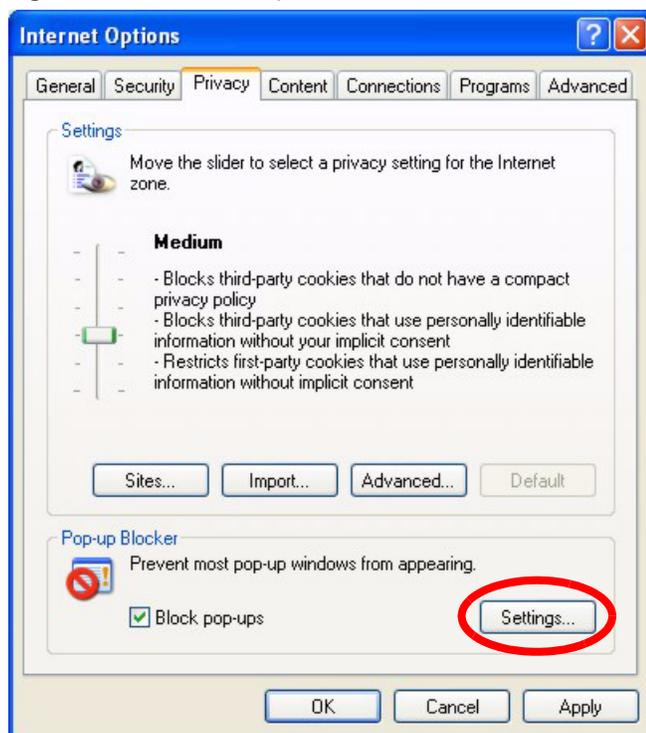
Figure 144 Internet Options

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

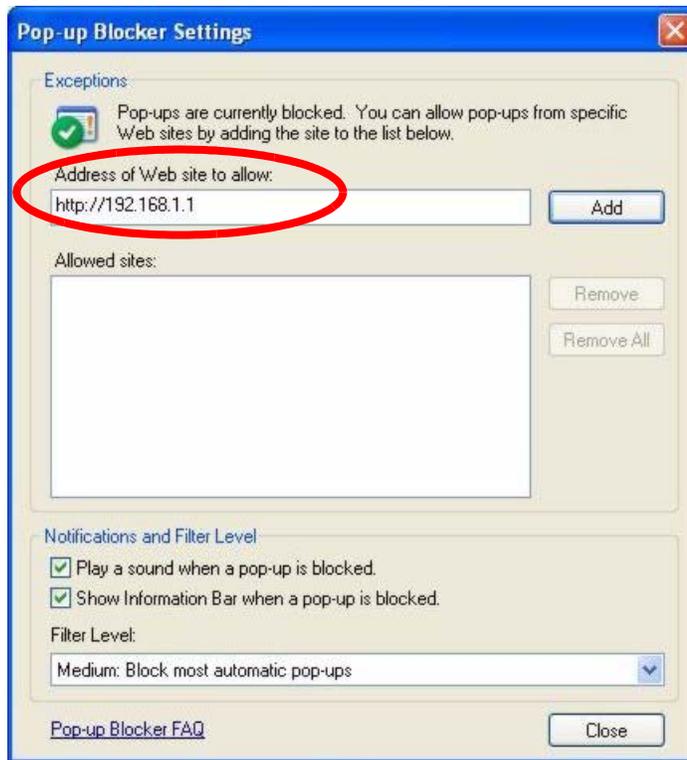
24.4.1.1.2 Enable pop-up Blockers with Exceptions

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 145 Internet Options

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

Figure 146 Pop-up Blocker Settings

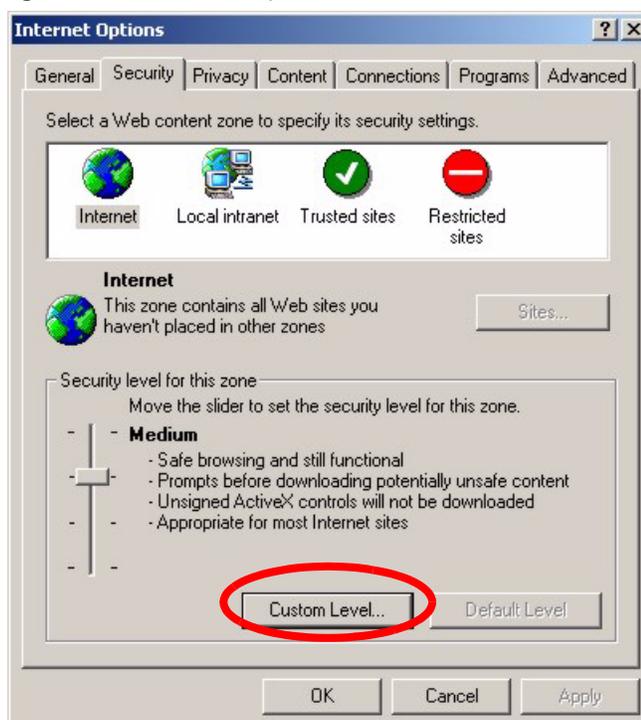
5 Click **Close** to return to the **Privacy** screen.

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

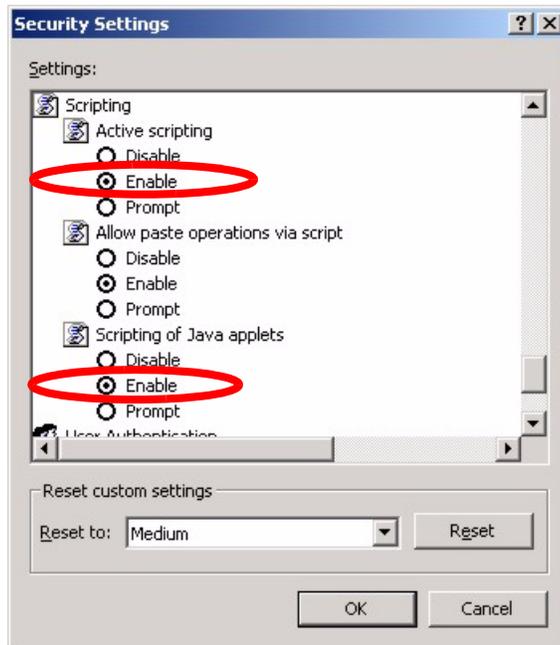
24.4.1.2 JavaScripts

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.

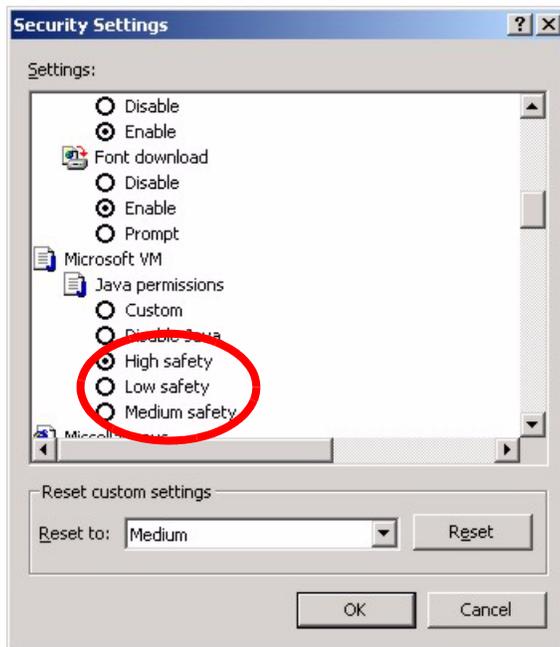
Figure 147 Internet Options

- 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 148 Security Settings - Java Scripting

24.4.1.3 Java Permissions

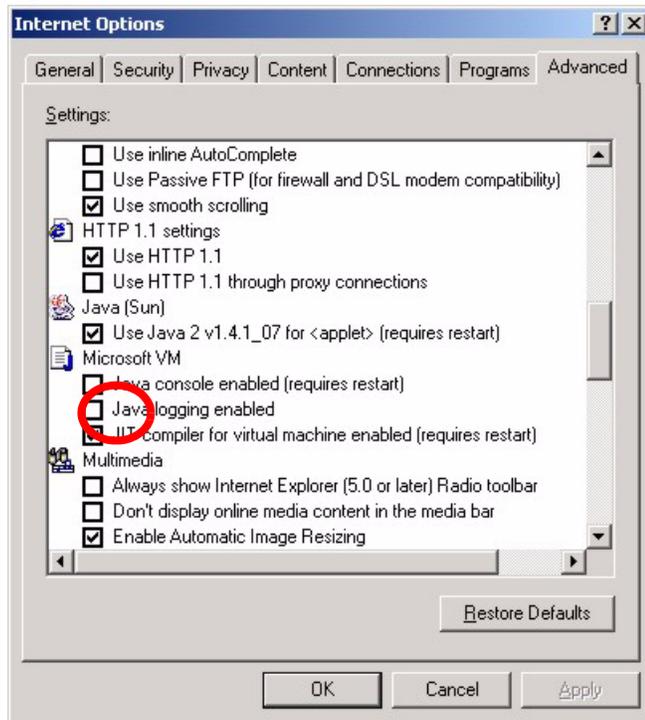
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 149 Security Settings - Java

24.4.1.3.1 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 150 Java (Sun)



24.5 Telephone Problems

Table 98 Troubleshooting Telephone

PROBLEM	CORRECTIVE ACTION
The telephone port won't work or the telephone lacks a dial tone.	Check the telephone connections and telephone wire. Make sure you have the VoIP SIP Settings screen properly configured.
I can access the Internet, but cannot make VoIP calls.	Make sure you have the VoIP SIP Settings screen properly configured. One of the PHONE lights should come on. Make sure that your telephone is connected to the corresponding PHONE port. You can also check the VoIP status in the Status screen. If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.
I cannot call from one of the ZyXEL Device's phone ports to the other phone port.	You cannot call the SIP number of the SIP account that you are using to make a call. The ZyXEL Device generates a busy tone and does not attempt to establish a call if the SIP number you dial matches the outgoing SIP number of the phone port you are using. For example, if you set Phone 1 to use SIP account 1 and set Phone 2 to use SIP account 2, then you can use Phone 1 to call to SIP account 2's SIP number or Phone 2 to call to SIP account 1's SIP number.

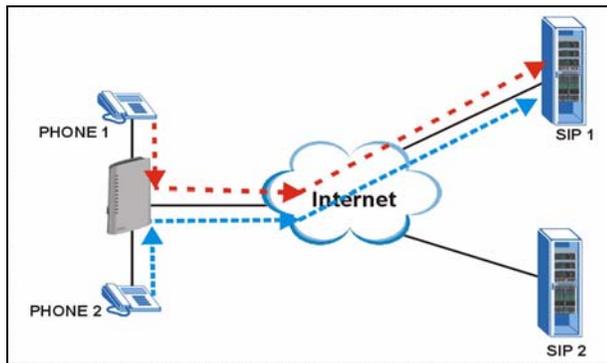
24.6 Problems With Multiple SIP Accounts

You can set up two SIP accounts on your ZyXEL Device and your ZyXEL Device is equipped with two phone ports. By default your ZyXEL Device uses SIP account 1 with both phone ports for outgoing calls and it uses SIP accounts 1 and 2 for incoming calls. With this setting, you always use SIP account 1 for your outgoing calls and you cannot distinguish which SIP account the calls are coming in through. If you want to control the use of different dialing plans for accounting purposes or other reasons, you need to configure your phone ports in order to control which SIP account you are using when placing or receiving calls.

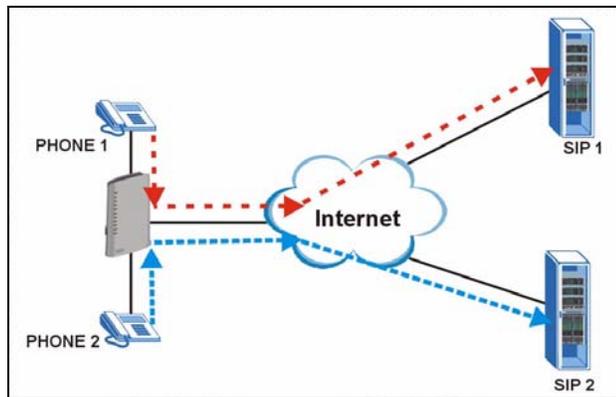
24.6.1 Outgoing Calls

The following figure represents the default behavior of your ZyXEL Device when two SIP accounts are configured and you are using two phones. When you place a call from phone 1 or phone 2, the ZyXEL Device will use SIP account 1.

Figure 151 Outgoing Calls: Both Phone Ports - SIP1

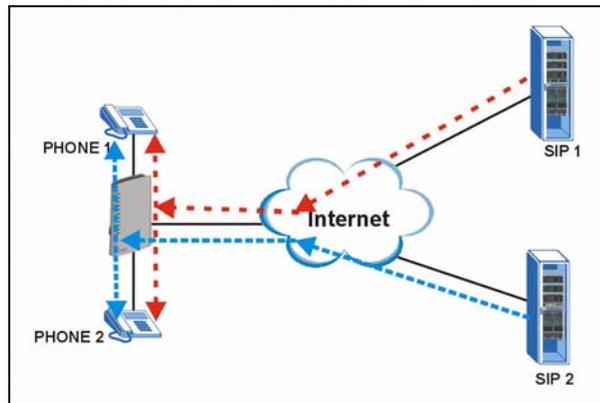


In the following figure phone port 1 is configured to use SIP account 1 and phone port 2 is configured to use SIP account 2. In this case, every time you place a call through phone port 1, you are using your SIP account 1. Similarly, every time you place a call through phone port 2, you are using your SIP account 2.

Figure 152 Outgoing Calls: Individual SIP Accounts

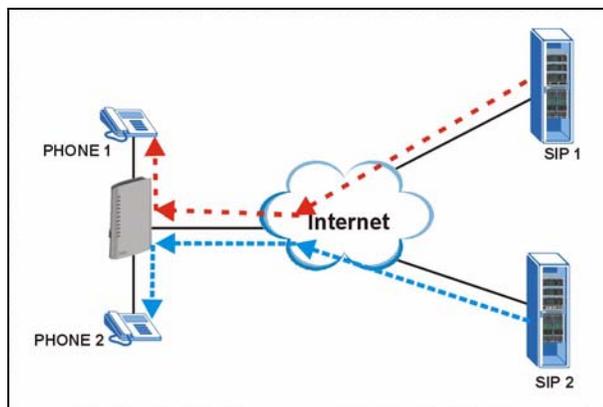
24.6.2 Incoming Calls

The following figure represents the default behavior of your ZyXEL Device when two SIP accounts are configured and you are using two phones. When a call comes in from your SIP account 1, the phones connected to both phone port 1 and phone port 2 ring. Similarly, when a call comes in from your SIP account 2, the phones connected to both phone port 1 and phone port 2 ring. In either case you are not sure which SIP account the call is coming from.

Figure 153 Incoming Calls: Both SIP Accounts

In the following figure phone port 1 is configured to use SIP account 1 and phone port 2 is configured to use SIP account 2 for incoming calls. In this case, every time you receive a call from your SIP account 1, the phone connected to phone port 1 rings. Similarly, every time you receive a call from your SIP account 2, the phone connected to phone port 2 rings.

Figure 154 Incoming Calls: Individual SIP Accounts



Appendix A

Product Specifications

See also [Chapter 1 on page 35](#) for a general overview of the key features.

Specification Tables

Table 99 Device Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Server IP Pool	192.168.1.33 to 192.168.1.65
Static DHCP Addresses	10
Dimensions	124mm(L) * 52mm(D) * 180mm(H)
Weight	317 g
Power Specification	12VAC 1A
Ethernet	1 auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
PHONE Ports	2 RJ-11 FXS POTS ports
LINE Port	1 RJ-11 FXO POTS port for PSTN calls ("L" models)
RESET Button	Restores factory defaults
Operation Temperature	0° C ~ 40° C
Storage Temperature	0° ~ 60° C
Operation Humidity	10% ~ 85% RH
Storage Humidity	10% ~ 90% RH

Table 100 Firmware Specifications

ADSL Standards	<p>Support ITU G.992.1 G.dmt (Annex A, Annex B, U-R2) EOC specified in ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL 2/2+ AnnexM ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC 2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) Multiple PPPoE VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) F4/F5 OAM Zero configuration</p>
Other Protocol Support	<p>PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols DHCP Server/Client/Relay RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy UPnP</p>
Management	<p>Embedded Web Configurator CLI (Command Line Interpreter) SNMP v1 & v2c with MIB II Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore Telnet for remote management Remote Management Control: Telnet, FTP, Web, SNMP and DNS. VoIP Auto-provisioning via TFTP / HTTP Remote Firmware Upgrade Syslog</p>
Firewall	<p>SPI Firewall Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc. Access Control of Service Content Filtering IP & Generic Packet Filtering Real time Attack Alerts and Logs Reports and logs SIP ALG passthrough</p>

Table 100 Firmware Specifications (continued)

NAT/SUA	Port Forwarding 512 NAT sessions per host Multimedia application PPTP under NAT/SUA IPSec passthrough SIP ALG passthrough
Content Filtering	Web page blocking by URL keyword.
Static Routes	16 IP
Voice Features	SIP version 2 (Session Initiating Protocol RFC 3261) SDP (Session Description Protocol RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) Voice codecs (coder/decoders) G.711 (a-law and μ -law), G.729 a/b G.168 echo cancellation (8ms ~ 16ms) Fax and data modem discrimination Silence Suppression / Voice Activity Detection (VAD) Comfort Noise Generation (CNG) Dynamic Jitter Buffer DTMF Detection and Generation DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO) Point-to-point call establishment between two IADs Quick dialing through predefined phone book, which maps the phone dialing number and destination URL. Multiple SIP number registration and multiple signaling handling capability.(per POTS port) Caller ID support Flexible Dial Plan (RFC3525 section 7.1.14) Multiple SIP Accounts / Phone Numbers- Freely assignable Numbers to Each Phone Port
Other Features	Any IP Zero Configuration (VC auto-hunting) Traffic Redirect Dynamic DNS IP Alias IP Policy Routing SPTGEN QoS

Power Adaptor Specifications

Table 101 ZyXEL Device Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACS
Input Power	AC120Volts/60Hz/23W max
Output Power	AC12Volts/1.0A

Table 101 ZyXEL Device Power Adaptor Specifications (continued)

Power Consumption	11 Watt
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
AC Power Adapter Model	AA-121A
Input Power	AC120Volts/60Hz/18W max
Output Power	AC12Volts/1.0A
Power Consumption	11 Watt
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
CHINA PLUG STANDARDS	
AC Power Adapter Model	AA-121AP
Input Power	AC220Volts/50Hz
Output Power	AC12Volts/1.0A
Power Consumption	11 Watt
Safety Standards	CCC (GB4943)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACUP-5716
Input Power	AC230Volts/50Hz/100mA
Output Power	AC12Volts/1.0A
Power Consumption	11 Watt
Safety Standards	TUV-GS, CE (EN 60950-1)
AC Power Adapter Model	AA-121ABN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	11 Watt
Safety Standards	ITS-GS, CE (EN 60950)
UNITED KINGDOM PLUG STANDARDS	
AC Power Adapter Model	AA-121AD
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	11 Watt
Safety Standards	ITS-GS, CE (EN 60950, BS 7002)
AUSTRALIA PLUG STANDARDS	
AC Power Adapter Model	AA-121AE
Input Power	AC240Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	11 Watt
Safety Standards	(AS/NZS 60950: 2000)

APPENDIX B

Splitters and Microfilters

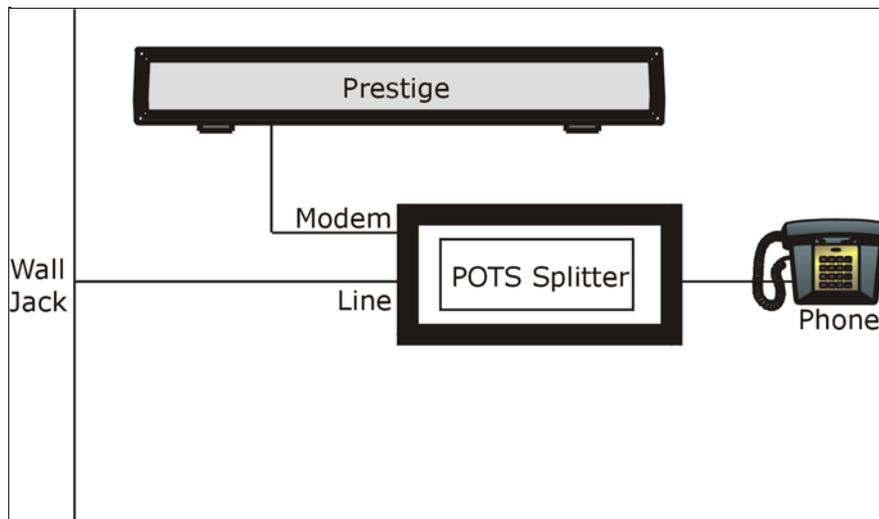
This appendix tells you how to install a POTS splitter or a telephone microfilter.

Connecting a POTS Splitter

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

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

Figure 155 Connecting a POTS Splitter



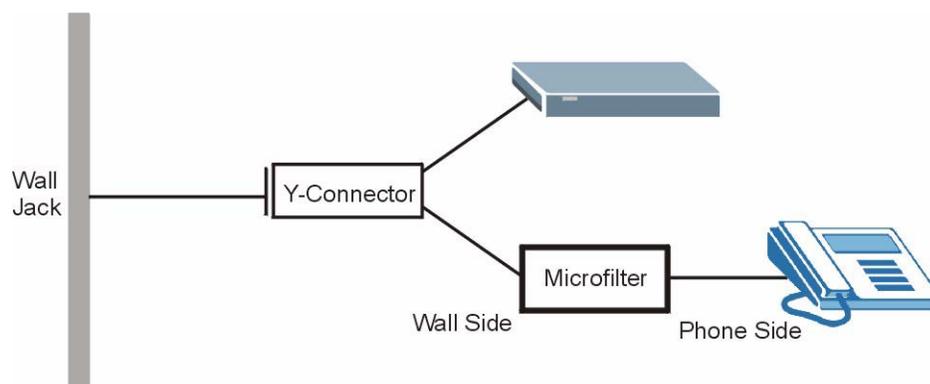
- 1 Connect the side labeled “Phone” to your telephone.
- 2 Connect the side labeled “Modem” or “DSL” to your ZyXEL Device.
- 3 Connect the side labeled “Line” to the telephone wall jack.

Telephone Microfilters

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

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

Figure 156 Connecting a Microfilter



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.

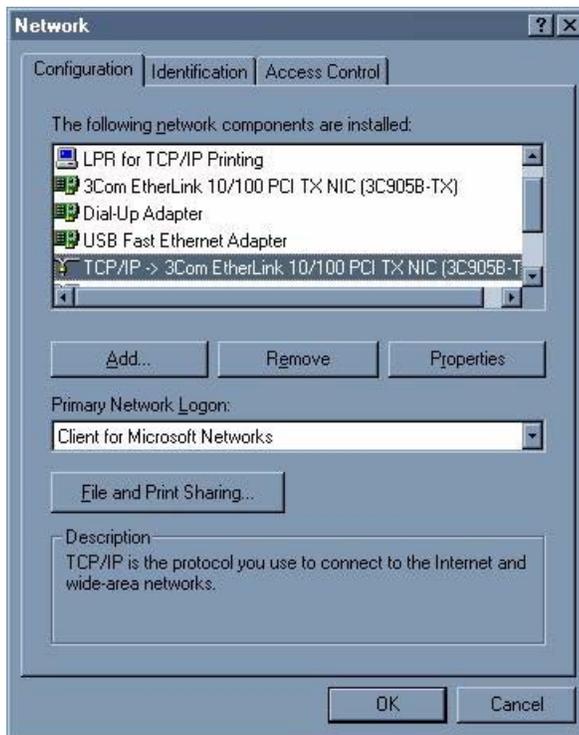
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 157 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:

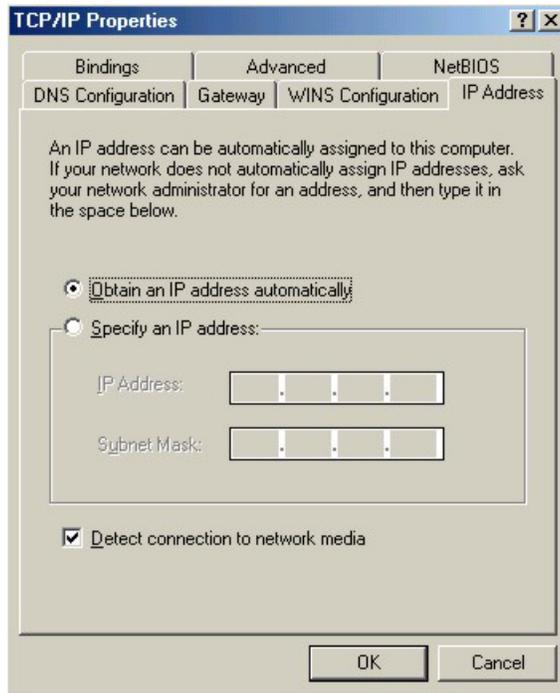
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

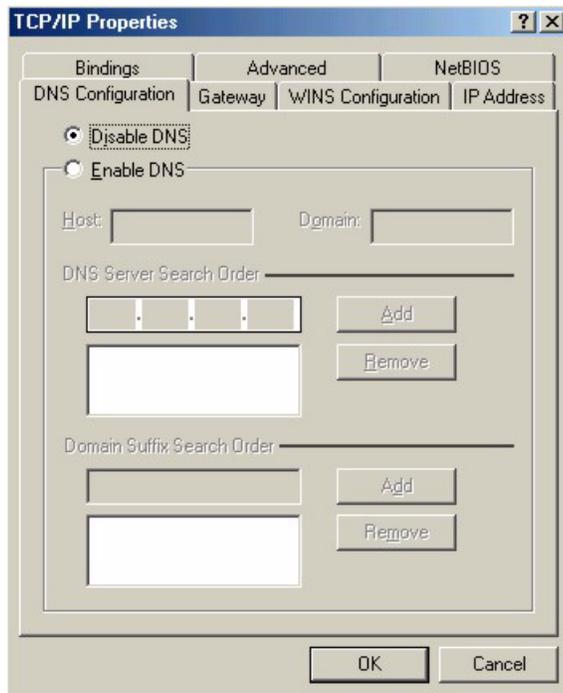
Configuring

- 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 158 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 159 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

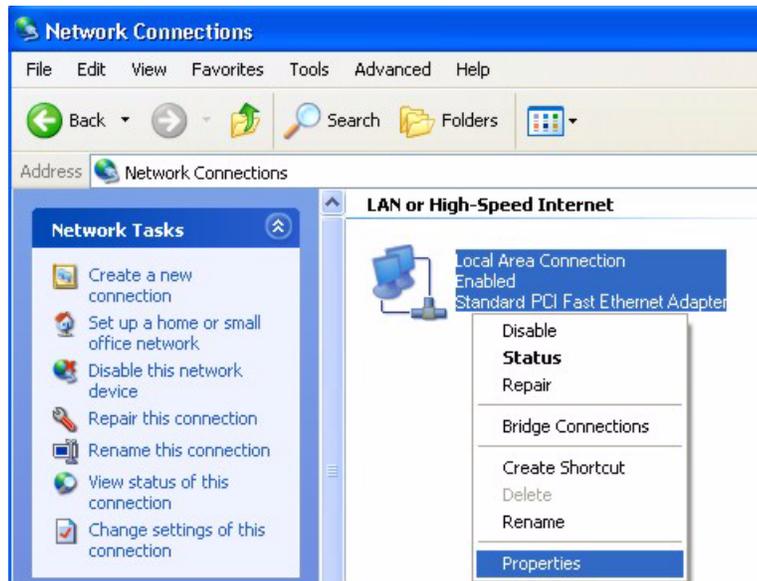
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 160 Windows XP: Start Menu

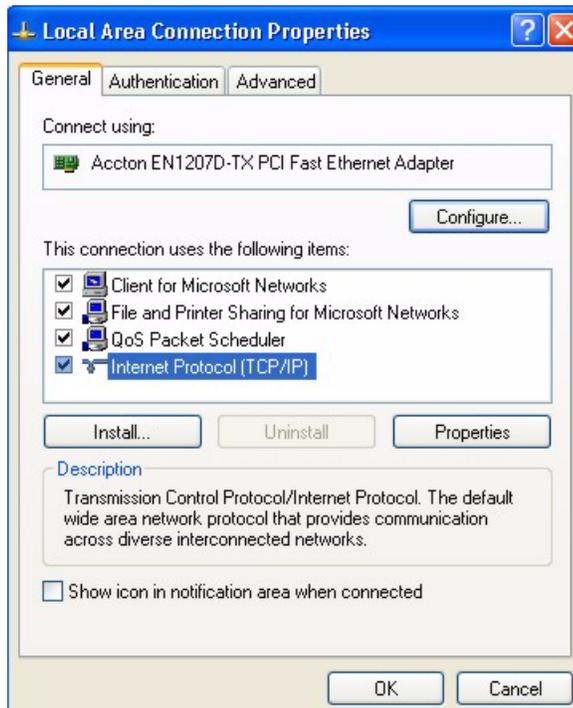
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 161 Windows XP: Control Panel

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

Figure 162 Windows XP: Control Panel: Network Connections: Properties

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

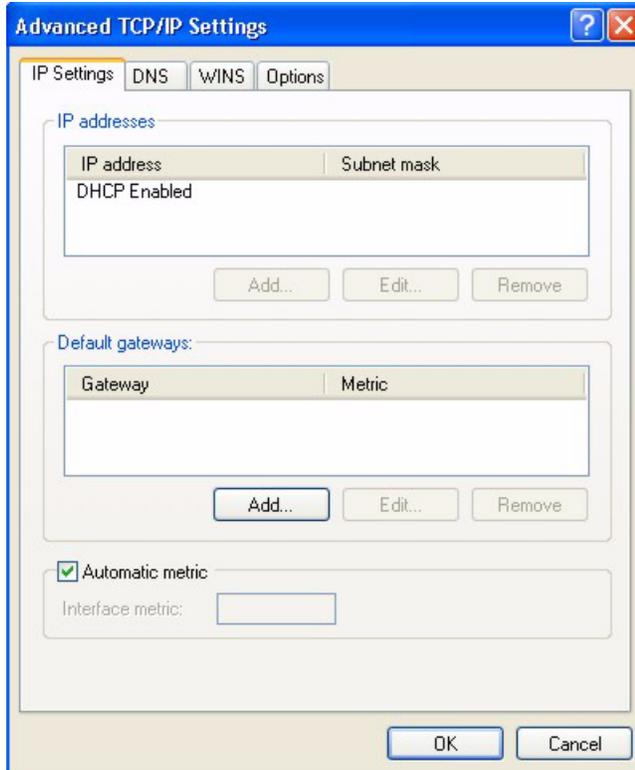
Figure 163 Windows XP: Local Area Connection Properties

- 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 164 Windows XP: Advanced TCP/IP Settings



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

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

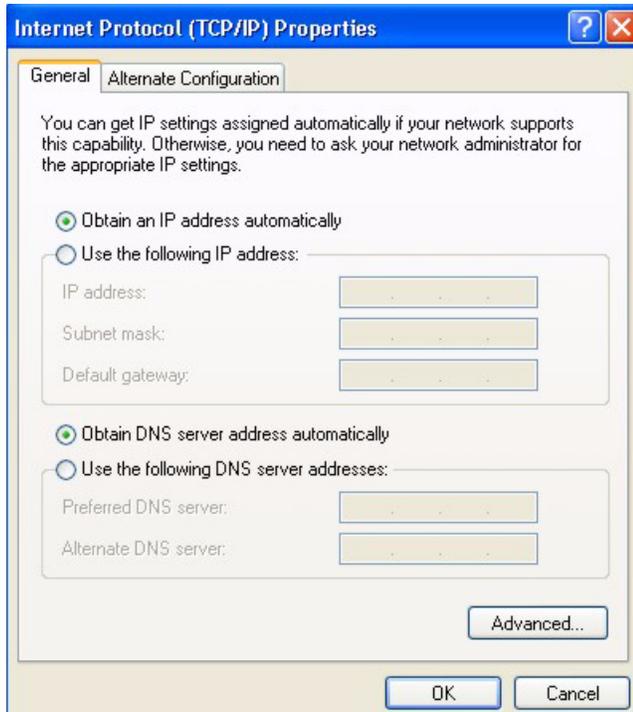
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP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

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

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

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

Figure 165 Windows XP: Internet Protocol (TCP/IP) Properties



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

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

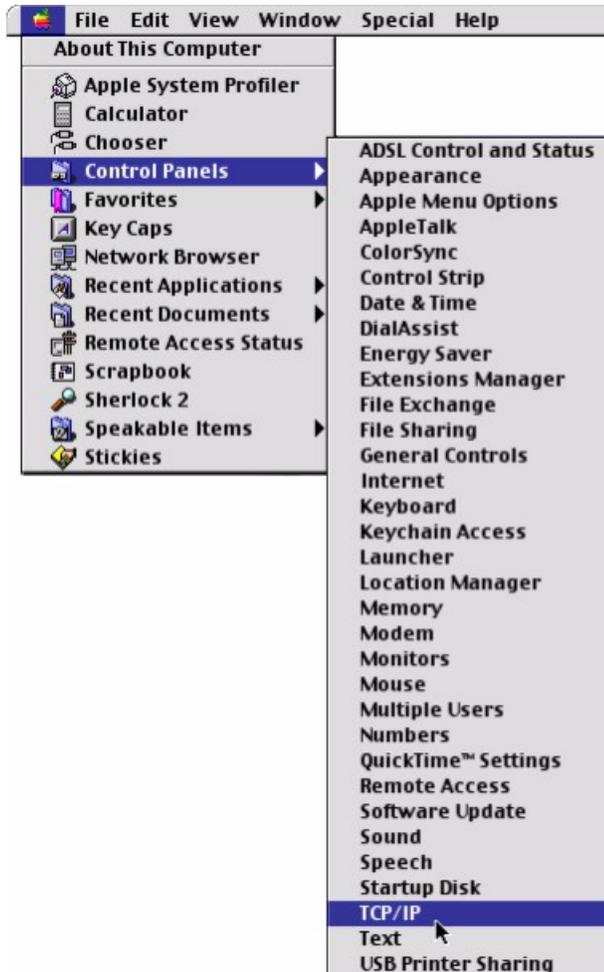
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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.

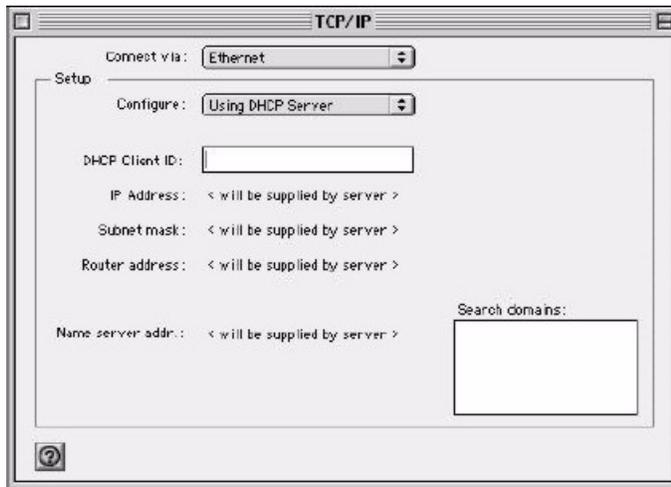
Macintosh OS 8/9

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

Figure 166 Macintosh OS 8/9: Apple Menu



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

Figure 167 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.

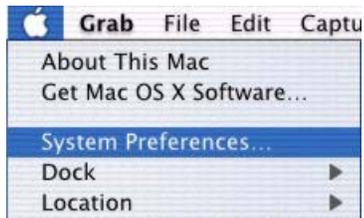
7 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

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

Macintosh OS X

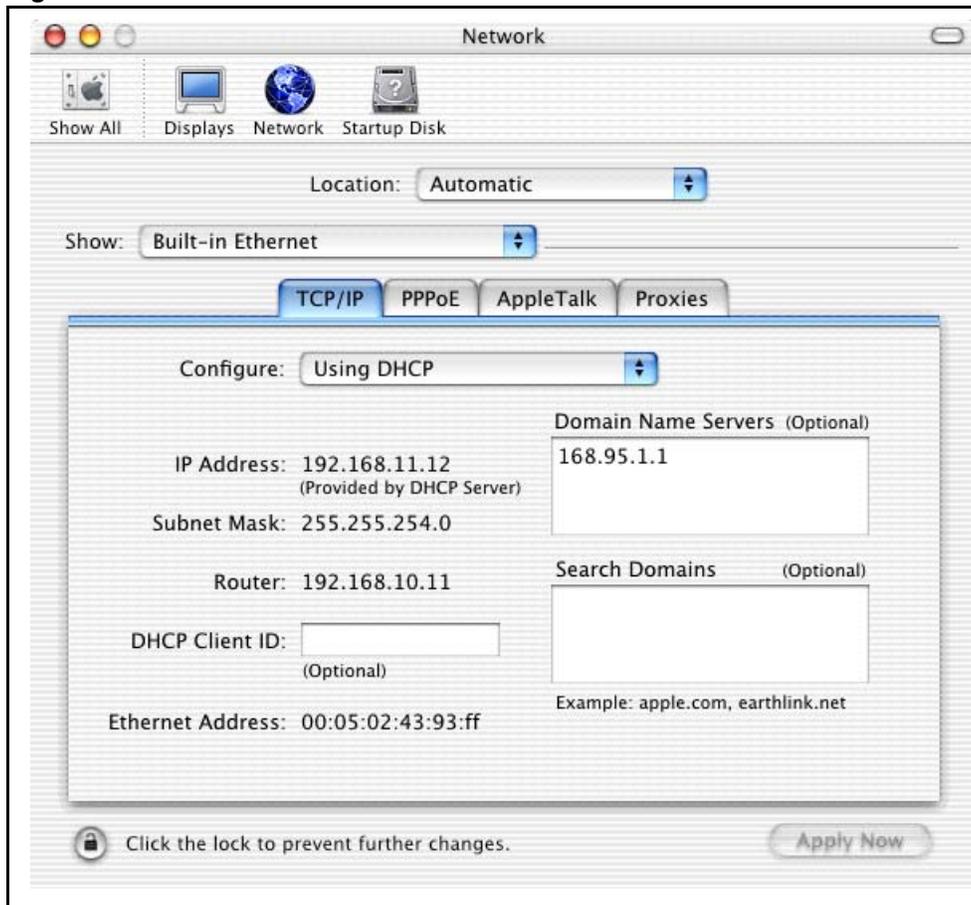
1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 168 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 169 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.

APPENDIX D

IP Subnetting

IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

Table 102 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class “C” network (8 host bits) can have $2^8 - 2$ or 254 hosts.

A class “B” address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class “A” address (24 host bits) can have $2^{24} - 2$ hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Table 103 Allowed IP Address Range By Class

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

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 is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

Table 104 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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

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

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

Table 105 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

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

Example: Two Subnets

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

Table 106 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”). You want to have two separate networks.

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

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

Table 107 Subnet 1

	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
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 108 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	

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

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

Table 109 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 110 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 111 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 112 Subnet 4

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

Example Eight Subnets

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

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

Table 113 Eight Subnets

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

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

Table 114 Class C Subnet Planning

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

Subnetting With Class A and Class B Networks.

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

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets ([Table 102 on page 285](#)) available for subnetting.

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

Table 115 Class B Subnet Planning

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

Appendix E

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 116 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.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

Table 116 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
RCMD	TCP	512	Remote Command Service.

Table 116 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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 F

Firewall Commands

Sys Firewall Commands

The following describes the firewall commands. See the Command Interpreter appendix for information on the command structure. Each of these commands must be preceded by `sys firewall` when you use them. For example, type `sys firewall active yes` to turn on the firewall.

Table 117 Sys Firewall Commands

Command		Description
acl		
	disp	Displays ACLs or a specific ACL set # and rule #.
active	<yes no>	Active firewall or deactivate firewall Enables/disables the firewall.
cnt		
	disp	Displays the firewall log type and count.
	clear	Clears the firewall log count.
pktdump		Dumps the last 64 bytes of packets that the firewall has dropped.
dynamicrule	display	Displays the firewall's dynamic rules.
tcprst		
	rst	Turns TCP reset sending on/off.
	rst113	Turns TCP reset sending for port 113 on/off.
	display	Displays the TCP reset sending settings.
icmp		This rule is not in use.
dos		
	smtp	Enables/disables the SMTP DoS defender.
	display	Displays the SMTP DoS defender setting.
	ignore	Sets if the firewall will ignore DoS attacks on the lan/wan.
ignore		
	dos	Sets if the firewall will ignore DoS attacks on the lan/wan.
	triangle	Sets if the firewall will ignore triangle route packets on the lan/wan.

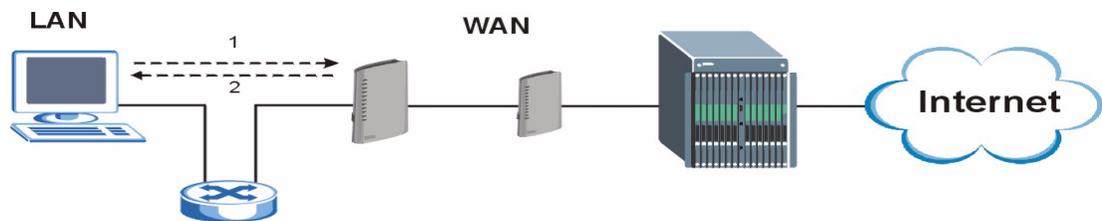
APPENDIX G

Triangle Route

The Ideal Setup

When the firewall is on, your ZyXEL Device acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyXEL Device to protect your LAN against attacks.

Figure 170 Ideal Setup



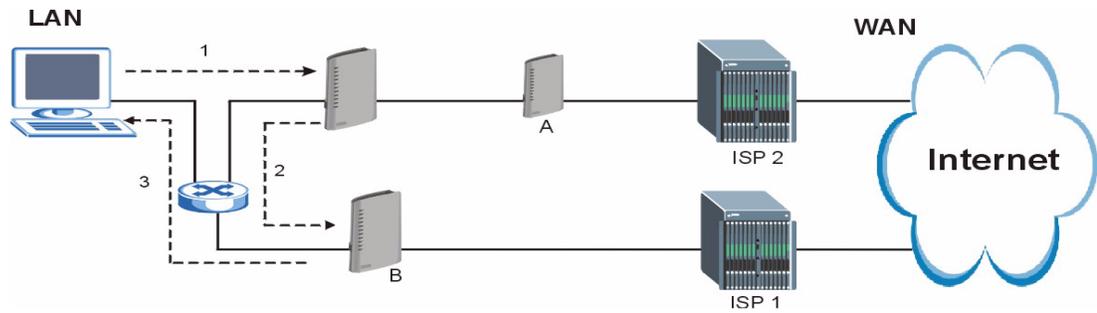
The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

- 1** A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2** The ZyXEL Device reroutes the SYN packet through Gateway **B** on the LAN to the WAN.
- 3** The reply from the WAN goes directly to the computer on the LAN without going through the ZyXEL Device.

As a result, the ZyXEL Device resets the connection, as the connection has not been acknowledged.

Figure 171 “Triangle Route” Problem



The “Triangle Route” Solutions

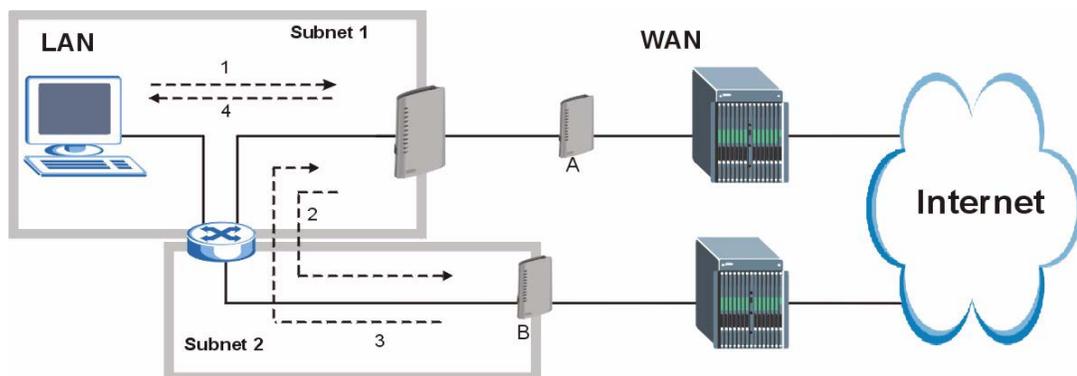
This section presents you two solutions to the “triangle route” problem.

IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyXEL Device supports up to three logical LAN interfaces with the ZyXEL Device being the gateway for each logical network. By putting your LAN and Gateway **B** 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 B, which is in Subnet 2.
- 3** The reply from WAN goes through the ZyXEL Device to the computer on the LAN in Subnet 1.

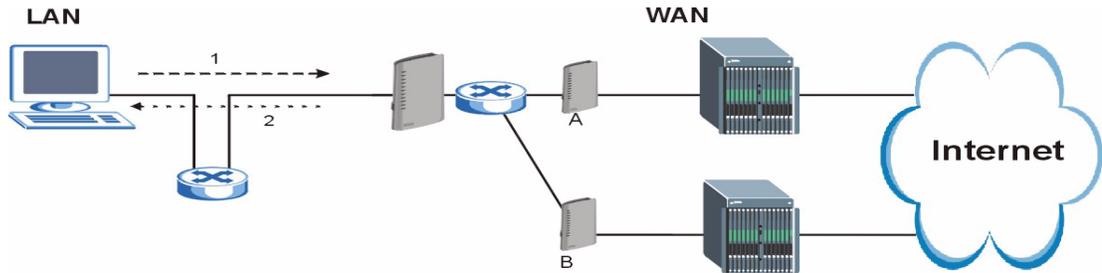
Figure 172 IP Alias



Gateways on the WAN Side

A second solution to the “triangle route” problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your ZyXEL Device to your LAN. Therefore your LAN is protected.

Figure 173 Gateways on the WAN Side



APPENDIX H

Log Descriptions

This appendix provides descriptions of example log messages.

Table 118 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 118 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 119 System Error Logs

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

Table 120 Access Control Logs

LOG MESSAGE	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 121 TCP Reset Logs

LOG MESSAGE	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. Default timeout values: ICMP idle timeout (s): 60 UDP idle timeout (s): 60 TCP connection (three way handshaking) timeout (s): 30 TCP FIN-wait timeout (s): 60 TCP idle (established) timeout (s): 3600
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 122 Packet Filter Logs

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

For type and code details, see [Table 131 on page 309](#).

Table 123 ICMP Logs

LOG MESSAGE	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.
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.

Table 123 ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
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 124 CDR Logs

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

Table 125 PPP Logs

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

Table 126 UPnP Logs

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

Table 127 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: block keyword	The content of a requested web page matched a user defined keyword.
%s	The system forwarded web content.

For type and code details, see [Table 131 on page 309](#).

Table 128 Attack Logs

LOG MESSAGE	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.
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.
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.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
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.
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.

Table 128 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
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.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.

Table 129 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user`s credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication method.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.

Table 129 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 130 ACL Setting Notes

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

Table 131 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

Table 131 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
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
	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 132 Syslog Logs

LOG MESSAGE	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>

Table 133 SIP Logs

LOG MESSAGE	DESCRIPTION
SIP Registration Success by SIP:SIP Phone Number	The listed SIP account was successfully registered with a SIP register server.
SIP Registration Fail by SIP:SIP Phone Number	An attempt to register the listed SIP account with a SIP register server was not successful.
SIP UnRegistration Success by SIP:SIP Phone Number	The listed SIP account's registration was deleted from the SIP register server.
SIP UnRegistration Fail by SIP:SIP Phone Number	An attempt to delete the listed SIP account's registration from the SIP register server failed.

Table 134 RTP Logs

LOG MESSAGE	DESCRIPTION
Error, RTP init fail	The initialization of an RTP session failed.
Error, Call fail: RTP connect fail	A VoIP phone call failed because the RTP session could not be established.
Error, RTP connection cannot close	The termination of an RTP session failed.

Table 135 FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
VoIP Call Established Ph[Phone Port] -> Outgoing Call Number	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
VoIP Call End Phone[Phone Port]	A VoIP phone call made from a phone connected to the listed phone port has terminated.

Table 136 FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start from SIP[SIP Port Number]	A VoIP phone call came to the ZyXEL Device from the listed SIP number.
VoIP Call Established Ph[Phone Port] <- Outgoing Call Number	A VoIP phone call was set up from the listed SIP number to the ZyXEL Device.
VoIP Call End Phone[Phone Port]	A VoIP phone call that came into the ZyXEL Device has terminated.

Table 137 Lifeline Logs

LOG MESSAGE	DESCRIPTION
PSTN Call Start	A PSTN call has been initiated.
PSTN Call End	A PSTN call has terminated.
PSTN Call Established	A PSTN call has been set up.

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

Table 138 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	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

Go to the command interpreter interface ([Appendix I on page 315](#) 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 174 Displaying Log Categories Example

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          ether          wan
ip           bridge         lan
dsp         voiceradius
ras>
```

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

Figure 175 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both]
ras>
```

- 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.

Figure 176 Log Command Example

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access
# .time                source                destination            notes
message
7|01/01/2000 09:40:13 |192.168.1.1:3         |192.168.1.33:1       |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
8|01/01/2000 09:40:07 |192.168.1.1:3         |192.168.1.33:1       |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
9|01/01/2000 09:40:04 |192.168.1.1:3         |192.168.1.33:1       |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
10|01/01/2000 09:40:04 |192.168.1.33:1199    |207.69.188.186:110   |ACCESS FO
RWARD
Firewall default policy: TCP (L to W)
11|01/01/2000 09:40:04 |192.168.1.1:53       |192.168.1.33:1200    |ACCESS FO
RWARD
none: UDP
```

APPENDIX I

Command Interpreter

The following describes how to use the command interpreter. Telnet to the ZyXEL Device and enter the password to use the commands. 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.

Command Syntax

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

For example,

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

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

Command Usage

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

APPENDIX J

Internal SPTGEN

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.

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 177 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 177 on page 317](#)), 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 178 on page 318](#), 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 177 on page 317](#)).

Figure 178 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 179 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 180 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 181 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 Screens

This section covers ZyXEL Device Internal SPTGEN screens.

Table 139 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number
FN	Field Name

Table 139 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the ZyXEL Device.

The following are the Internal SPTGEN menus.

Table 140 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 141 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
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			

Table 141 Menu 3

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
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

Table 141 Menu 3

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				
	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

Table 141 Menu 3

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
*/ 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 142 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

Table 142 Menu 4 Internet Access Setup (continued)

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 (D ynamic)>	= 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
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

Table 142 Menu 4 Internet Access Setup (continued)

40000032=	RIP Version	<0 (Rip-1) 1 (Rip-2B) 2 (Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0 (No) 1 (Yes)>	= 0

Table 143 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
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0 (No) 1 (Yes)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask		= 0
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		= 0
120102007 =	IP Static Route set #2, Private	<0 (No) 1 (Yes)>	= 0
/ Menu 12.1.3 IP Static Route Setup			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name	<Str>	=
120103002 =	IP Static Route set #3, Active	<0 (No) 1 (Yes)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0 (No) 1 (Yes)>	= 0

Table 143 Menu 12 (continued)

/ Menu 12.1.4 IP Static Route Setup			
FIN	FN	PVA	INPUT
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0 (No) 1 (Yes)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0
120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0 (No) 1 (Yes)>	= 0
/ Menu 12.1.5 IP Static Route Setup			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0 (No) 1 (Yes)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0
120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0 (No) 1 (Yes)>	= 0
/ Menu 12.1.6 IP Static Route Setup			
FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0 (No) 1 (Yes)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0 (No) 1 (Yes)>	= 0
/ Menu 12.1.7 IP Static Route Setup			
FIN	FN	PVA	INPUT
120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0 (No) 1 (Yes)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0

Table 143 Menu 12 (continued)

120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(No) 1(Yes)>	= 0
/ Menu 12.1.8 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
*/ Menu 12.1.9 IP Static Route Setup			
FIN	FN	PVA	INPUT
120109001 =	IP Static Route set #9, Name	<Str>	=
120109002 =	IP Static Route set #9, Active	<0(No) 1(Yes)>	= 0
120109003 =	IP Static Route set #9, Destination IP address		= 0.0.0.0
120109004 =	IP Static Route set #9, Destination IP subnetmask		= 0
120109005 =	IP Static Route set #9, Gateway		= 0.0.0.0
120109006 =	IP Static Route set #9, Metric		= 0
120109007 =	IP Static Route set #9, Private	<0(No) 1(Yes)>	= 0
*/ Menu 12.1.10 IP Static Route Setup			
FIN	FN	PVA	INPUT
120110001 =	IP Static Route set #10, Name		=
120110002 =	IP Static Route set #10, Active	<0(No) 1(Yes)>	= 0
120110003 =	IP Static Route set #10, Destination IP address		= 0.0.0.0
120110004 =	IP Static Route set #10, Destination IP subnetmask		= 0
120110005 =	IP Static Route set #10, Gateway		= 0.0.0.0
120110006 =	IP Static Route set #10, Metric		= 0
120110007 =	IP Static Route set #10, Private	<0(No) 1(Yes)>	= 0
*/ Menu 12.1.11 IP Static Route Setup			
FIN	FN	PVA	INPUT
120111001 =	IP Static Route set #11, Name	<Str>	=
120111002 =	IP Static Route set #11, Active	<0(No) 1(Yes)>	= 0
120111003 =	IP Static Route set #11, Destination IP address		= 0.0.0.0

Table 143 Menu 12 (continued)

120111004 =	IP Static Route set #11, Destination IP subnetmask		= 0
120111005 =	IP Static Route set #11, Gateway		= 0.0.0.0
120111006 =	IP Static Route set #11, Metric		= 0
120111007 =	IP Static Route set #11, Private	<0 (No) 1 (Yes)>	= 0
*/ Menu 12.1.12 IP Static Route Setup			
FIN	FN	PVA	INPUT
120112001 =	IP Static Route set #12, Name	<Str>	=
120112002 =	IP Static Route set #12, Active	<0 (No) 1 (Yes)>	= 0
120112003 =	IP Static Route set #12, Destination IP address		= 0.0.0.0
120112004 =	IP Static Route set #12, Destination IP subnetmask		= 0
120112005 =	IP Static Route set #12, Gateway		= 0.0.0.0
120112006 =	IP Static Route set #12, Metric		= 0
120112007 =	IP Static Route set #12, Private	<0 (No) 1 (Yes)>	= 0
*/ Menu 12.1.13 IP Static Route Setup			
FIN	FN	PVA	INPUT
120113001 =	IP Static Route set #13, Name	<Str>	=
120113002 =	IP Static Route set #13, Active	<0 (No) 1 (Yes)>	= 0
120113003 =	IP Static Route set #13, Destination IP address		= 0.0.0.0
120113004 =	IP Static Route set #13, Destination IP subnetmask		= 0
120113005 =	IP Static Route set #13, Gateway		= 0.0.0.0
120113006 =	IP Static Route set #13, Metric		= 0
120113007 =	IP Static Route set #13, Private	<0 (No) 1 (Yes)>	= 0
*/ Menu 12.1.14 IP Static Route Setup			
FIN	FN	PVA	INPUT
120114001 =	IP Static Route set #14, Name	<Str>	=
120114002 =	IP Static Route set #14, Active	<0 (No) 1 (Yes)>	= 0
120114003 =	IP Static Route set #14, Destination IP address		= 0.0.0.0
120114004 =	IP Static Route set #14, Destination IP subnetmask		= 0
120114005 =	IP Static Route set #14, Gateway		= 0.0.0.0
120114006 =	IP Static Route set #14, Metric		= 0
120114007 =	IP Static Route set #14, Private	<0 (No) 1 (Yes)>	= 0
*/ Menu 12.1.15 IP Static Route Setup			
FIN	FN	PVA	INPUT
120115001 =	IP Static Route set #15, Name	<Str>	=

Table 143 Menu 12 (continued)

120115002 =	IP Static Route set #15, Active	<0 (No) 1 (Yes)>	= 0
120115003 =	IP Static Route set #15, Destination IP address		= 0.0.0.0
120115004 =	IP Static Route set #15, Destination IP subnetmask		= 0
120115005 =	IP Static Route set #15, Gateway		= 0.0.0.0
120115006 =	IP Static Route set #15, Metric		= 0
120115007 =	IP Static Route set #15, Private	<0 (No) 1 (Yes)>	= 0
*/ Menu 12.1.16 IP Static Route Setup			
FIN	FN	PVA	INPUT
120116001 =	IP Static Route set #16, Name	<Str>	=
120116002 =	IP Static Route set #16, Active	<0 (No) 1 (Yes)>	= 0
120116003 =	IP Static Route set #16, Destination IP address		= 0.0.0.0
120116004 =	IP Static Route set #16, Destination IP subnetmask		= 0
120116005 =	IP Static Route set #16, Gateway		= 0.0.0.0
120116006 =	IP Static Route set #16, Metric		= 0
120116007 =	IP Static Route set #16, Private	<0 (No) 1 (Yes)>	= 0

Table 144 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

Table 144 Menu 15 SUA Server Setup (continued)

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
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

Table 144 Menu 15 SUA Server Setup (continued)

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 145 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
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

Table 145 Menu 21.1 Filter Set #1 (continued)

/ 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
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
/ Menu 21.1.1.3 set #1, rule #3			
FIN	FN	PVA	INPUT
210103001 =	IP Filter Set 1,Rule 3 Type	<2 (TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active	<0 (No) 1 (Yes)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port		= 139
210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address		= 0.0.0.0
210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0

Table 145 Menu 21.1 Filter Set #1 (continued)

210103013 =	IP Filter Set 1,Rule 3 Act Match	<1 (check next) 2 (forward) 3 (drop)	= 3
210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1 (check next) 2 (forward) 3 (drop)	= 1
/ Menu 21.1.1.4 set #1, rule #4			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type	<2 (TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0 (No) 1 (Yes)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1 (check next) 2 (forward) 3 (drop)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1 (check next) 2 (forward) 3 (drop)	= 1
/ Menu 21.1.1.5 set #1, rule #5			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type	<2 (TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active	<0 (No) 1 (Yes)>	= 1
210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0

Table 145 Menu 21.1 Filter Set #1 (continued)

210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match	<1 (Check Next) 2 (Forward) 3 (Drop)>	= 1
/ Menu 21.1.1.6 set #1, rule #6			
FIN	FN	PVA	INPUT
210106001 =	IP Filter Set 1,Rule 6 Type	<2 (TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0 (No) 1 (Yes)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139
210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210106013 =	IP Filter Set 1,Rule 6 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1 (check next) 2 (forward) 3 (drop)>	= 2

Table 146 Menu 21.1 Filer Set #2,

/ Menu 21.1 filter set #2,			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN

Table 146 Menu 21.1 Filer Set #2, (continued)

/ 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
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

Table 146 Menu 21.1 Filer Set #2, (continued)

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
/ Menu 21.1.2.3 Filter set #2, rule #3			
FIN	FN	PVA	INPUT
210203001 =	IP Filter Set 2, Rule 3 Type	<0 (none) 2 (TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active	<0 (No) 1 (Yes)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask		= 0
210203006 =	IP Filter Set 2, Rule 3 Dest Port		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address		= 0.0.0.0
210203009 =	IP Filter Set 2, Rule 3 Src Subnet Mask		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port		= 0
210203011 =	IP Filter Set 2, Rule 3 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210203013 =	IP Filter Set 2, Rule 3 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210203014 =	IP Filter Set 2, Rule 3 Act Not Match	<1 (check next) 2 (forward) 3 (drop)>	= 1
/ Menu 21.1.2.4 Filter set #2, rule #4			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type	<0 (none) 2 (TCP/IP)>	= 2

Table 146 Menu 21.1 Filer Set #2, (continued)

210204002 =	IP Filter Set 2, Rule 4 Active		<0 (No) 1 (Yes) > = 1
210204003 =	IP Filter Set 2, Rule 4 Protocol		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address		= 0.0.0.0
210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port		= 137
210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater) >	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater) >	= 0
210204013 =	IP Filter Set 2, Rule 4 Act Match	<1 (check next) 2 (forward) 3 (drop) >	= 3
210204014 =	IP Filter Set 2, Rule 4 Act Not Match	<1 (check next) 2 (forward) 3 (drop) >	= 1
/ Menu 21.1.2.5 Filter set #2, rule #5			
FIN	FN	PVA	INPUT
210205001 =	IP Filter Set 2, Rule 5 Type	<0 (none) 2 (TCP/IP) >	= 2
210205002 =	IP Filter Set 2, Rule 5 Active	<0 (No) 1 (Yes) >	= 1
210205003 =	IP Filter Set 2, Rule 5 Protocol		= 17
210205004 =	IP Filter Set 2, Rule 5 Dest IP address		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater) >	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port		= 0

Table 146 Menu 21.1 Filer Set #2, (continued)

210205011 =	IP Filter Set 2, Rule 5 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210205014 =	IP Filter Set 2, Rule 5 Act Not Match	<1 (check next) 2 (forward) 3 (drop)>	= 1
/ Menu 21.1.2.6 Filter set #2, rule #6			
FIN	FN	PVA	INPUT
210206001 =	IP Filter Set 2, Rule 6 Type	<0 (none) 2 (TCP/IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active	<0 (No) 1 (Yes)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol		= 17
210206004 =	IP Filter Set 2, Rule 6 Dest IP address		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp	<0 (none) 1 (equal) 2 (not equal) 3 (less) 4 (greater)>	= 0
210206013 =	IP Filter Set 2, Rule 6 Act Match	<1 (check next) 2 (forward) 3 (drop)>	= 3
210206014 =	IP Filter Set 2, Rule 6 Act Not Match	<1 (check next) 2 (forward) 3 (drop)>	= 2
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

Table 147 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
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 (WPAPSK)>	= 0
230400006 =	Dynamic WEP Key Exchange	<0 (Disable) 1 (64-bit WEP) 2 (128-bit WEP)>	= 0
230400007 =	PSK =		=

Table 147 Menu 23 System Menus (continued)

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 148 Menu 24.11 Remote Management Control

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

FIN	FN	PVA	INPUT
/ci command (for annex a): wan adsl opencmd			
990000001 =	ADSL OPMD	<0 (glite) 1 (t1.413) 2 (gdm) 3 (multimode)>	= 3
/ci command (for annex B): wan adsl opencmd			

Table 149 Command Examples (continued)

	FIN	FN	PVA	INPUT
	FIN	FN	PVA	INPUT
	990000001 =	ADSL OPMD	<0(etsi) 1(normal) 2(gdmt) 3(multimo de)>	= 3

Index

A

AAL5 [268](#)
 AbS [125](#)
 Address Assignment [97](#)
 Address Resolution Protocol (ARP) [100](#)
 ADSL Standards [36](#)
 ADSL2 [268](#)
 ALG [38, 117](#)
 Alternative Subnet Mask Notation [287](#)
 Analysis-by-Synthesis [125](#)
 Any IP [99](#)
 How it works [100](#)
 note [100](#)
 Any IP Setup [102](#)
 Application Layer Gateway [38, 117](#)
 Application-level Firewalls [150](#)
 Asynchronous Transfer Mode [250](#)
 ATM AAL5 [268](#)
 ATM Adaptation Layer 5 (AAL5) [82](#)
 ATM Adaptation Layer type 5 [268](#)
 Attack Alert [177](#)
 Attack Types [154](#)
 Auto Firmware Upgrade [37, 148](#)
 Automatic Log Out [47](#)
 Auto-negotiating Rate Adaptation [268](#)
 Auto-provisioning [37, 148](#)

B

Backup [239](#)
 Backup Type [94](#)
 Bandwidth Management [187](#)
 Bandwidth Manager Class Configuration [192](#)
 Bandwidth Manager Monitor [196](#)
 Bandwidth Manager Summary [191](#)
 Blocking Time [176](#)
 Brute-force Attack, [153](#)
 BW Budget [193](#)

C

Call Hold [138, 140](#)
 Call Service Mode [138, 139](#)
 Call Transfer [139, 140](#)
 Call Waiting [139, 140](#)
 Caller ID [269](#)
 CBR (Continuous Bit Rate) [90](#)
 Certifications [4](#)
 Viewing [4](#)
 Change Password [46](#)
 at Login [46](#)
 Checking the Device's IP Address [147](#)
 Class of Service [131](#)
 Class of Service (CoS) [131](#)
 Client-server Protocol [120](#)
 CNG [269](#)
 Codec [125](#)
 Codecs [269](#)
 Coder/Decoder [125](#)
 Comfort Noise Generation [38, 133, 269](#)
 Computer [34](#)
 Configuration File [235](#)
 Content Filtering [37, 179](#)
 Categories [179](#)
 Schedule [180](#)
 Trusted computers [181](#)
 URL keyword blocking [179](#)
 CoS [131](#)
 Custom Ports
 Creating/Editing [171](#)
 Customized Services [170](#)
 Customized services [170](#)

D

Default [240](#)
 Default LAN IP Address [45](#)
 Denial of Service [151, 176](#)
 Destination Address [163](#)
 DHCP [39, 96, 97, 197, 223](#)
 DHCP Client [39](#)
 DHCP Relay [39](#)

DHCP Server [39](#)
diagnostic [249](#)
Differentiated Services [131](#)
DiffServ [131](#)
DiffServ Code Point (DSCP) [131](#)
DiffServ Code Points [131](#)
DiffServ Marking Rule [132](#)
Disclaimer [3](#)
DNS [209](#)
DNS (Domain Name System) [96](#)
Domain Name [97](#), [114](#), [223](#)
DoS
 Basics [151](#)
 Types [152](#)
DoS (Denial of Service) [37](#)
DoS (Denial of Service), firewall [150](#)
DoS attacks, types of [152](#)
DS Field [131](#)
DSCPs [131](#)
DSL line, reinitialize [251](#)
DSLAM (Digital Subscriber Line Access Multiplexer) [40](#)
DTMF [126](#)
DTMF Detection and Generation [269](#)
Dual-Tone MultiFrequency [126](#)
Dynamic DNS [39](#), [197](#)
Dynamic Host Configuration Protocol [39](#)
Dynamic Jitter Buffer [37](#)
Dynamic Jitter Butter [269](#)
DYNDNS Wildcard [197](#)

E

ECHO [114](#)
Echo Cancellation [38](#), [134](#), [269](#)
E-mail
 Log Example [233](#)
Emergency Numbers [133](#)
Encapsulated Routing Link Protocol (ENET ENCAP) [81](#)
Encapsulation [81](#)
 ENET ENCAP [81](#)
 PPP over Ethernet [81](#)
 PPPoA [82](#)
 RFC 1483 [82](#)
Ethernet port, Auto-negotiation [36](#)
Europe Type Call Service Mode [138](#)

F

Fairness-based Scheduler [188](#)
FCC Interference Statement [4](#)
Filename Conventions [235](#), [236](#)
Finger [114](#)
Firewall
 Access Methods [161](#)
 Address Type [169](#)
 Alerts [164](#)
 Creating/Editing Rules [167](#)
 Custom Ports [170](#)
 Enabling [164](#)
 Firewall Vs Filters [159](#)
 Guidelines For Enhancing Security [158](#)
 Introduction [150](#)
 LAN to WAN Rules [164](#)
 Policies [161](#)
 Rule Checklist [162](#)
 Rule Logic [162](#)
 Rule Security Ramifications [162](#)
 Types [149](#)
 When To Use [160](#)
Firmware [235](#)
firmware [235](#)
 upload [236](#)
 upload error [238](#)
Flash Key [138](#)
Flashing [138](#)
Frame Relay [40](#)
FTP [114](#), [201](#), [204](#)
 File Upload [245](#)
FTP Restrictions [201](#), [236](#)
Full Rate [271](#)

G

G.168 [38](#), [134](#), [269](#)
G.711 [125](#), [269](#)
G.729 [125](#), [269](#)
G.992.1 [268](#)
G.992.3 [268](#)
G.992.4 [268](#)
G.992.5 [268](#)
General Setup [223](#)
Graphical User Interface (GUI) [36](#)
Graphics Icons [34](#)
Graphics Icons Key [34](#)

H

Half-Open Sessions [176](#)
 Host [224](#)
 Host IDs [285](#)
 Housing [39](#)
 HTTP [114](#), [151](#), [152](#)
 HTTP (Hypertext Transfer Protocol) [236](#)
 HTTP, firewall [150](#)
 Humidity [267](#)

I

IAD (Integrated Access Device) [35](#)
 IANA [98](#)
 IANA (Internet Assigned Number Authority) [170](#)
 ICMP echo [153](#)
 Icons Key [34](#)
 IEEE 802.1Q VLAN [132](#)
 IGMP [99](#)
 IGMP Proxy [268](#)
 IGMP v1 [268](#)
 IGMP v2 [268](#)
 Install UPnP [213](#)
 Windows Me [213](#)
 Windows XP [215](#)
 Internal Calls [147](#)
 Internal SPTGEN [317](#)
 FTP Upload Example [319](#)
 Points to Remember [317](#)
 Text File [317](#)
 Internet Access [36](#), [40](#), [53](#), [86](#)
 wizard setup [53](#)
 Internet Access Setup [254](#)
 Internet Assigned Numbers AuthoritySee IANA [98](#)
 Internet Control Message Protocol (ICMP) [153](#)
 Internet Telephony Service Provider [40](#)
 IP Address [97](#), [114](#), [115](#), [116](#)
 IP Address Assignment [83](#)
 ENET ENCAP [83](#)
 PPPoA or PPPoE [83](#)
 RFC 1483 [83](#)
 IP Addressing [285](#)
 IP Alias [39](#)
 IP Classes [285](#)
 IP Multicasting [268](#)
 IP Policy Routing (IPPR) [39](#)
 IP Pool [103](#)
 IP Spoofing [152](#), [155](#)

IP to IP Calls [41](#)
 IPSec Passthrough [269](#)
 ISDN (Integrated Services Digital Network) [35](#)
 ITSP [40](#)
 ITU-T [134](#)
 ITU-T G.992.1 [251](#)

K

Key Fields For Configuring Rules [163](#)

L

LAN Setup [81](#), [95](#)
 LAN TCP/IP [97](#)
 LAN to WAN Rules [164](#)
 LAND [152](#), [153](#)
 Listening Port [130](#)
 Log Out [47](#)
 Logs [229](#)

M

Management Information Base (MIB) [206](#)
 Maximize Bandwidth Usage [189](#)
 Maximum Burst Size (MBS) [85](#), [90](#)
 Max-incomplete High [176](#)
 Max-incomplete Low [176](#)
 Media Bandwidth Management [37](#)
 Metric [84](#)
 Modem [34](#)
 Multicast [99](#)
 Multimedia [119](#)
 Multiple PVC Support [39](#)
 Multiplexing [82](#)
 multiplexing [82](#)
 LLC-based [82](#)
 VC-based [82](#)
 Multiprotocol Encapsulation [82](#)

N

Nailed-Up Connection [83](#)

NAT [97](#), [114](#), [115](#)
 Application [111](#)
 Definitions [109](#)
 How it works [110](#)
 Mapping Types [111](#)
 Server Mode [111](#)
 What it does [110](#)
 What NAT does [110](#)
NAT (Network Address Translation) [37](#), [109](#)
NAT mode [113](#)
NAT Sessions [269](#)
NAT Traversal [211](#)
NetBIOS commands [154](#)
Network Management [114](#)
NNTP [114](#)
Notebook Computer [34](#)

O

OAM [268](#)
One-Minute High [176](#)
Operation Humidity [267](#)
Operation Temperature [267](#)

P

Packet Filtering [159](#)
Packet filtering
 When to use [160](#)
Packet Filtering Firewalls [149](#)
PCM [125](#)
Peak Cell Rate (PCR) [84](#), [90](#)
Peer to Peer Calls [41](#)
Per-Hop Behavior [131](#)
Permanent Virtual Circuits [268](#)
PHB (Per-Hop Behavior) [132](#)
Phone [133](#)
Ping of Death [152](#)
Point to Point Calls [41](#)
Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [82](#)
Point-to-point Calls [269](#)
Point-to-Point Tunneling Protocol [114](#)
POP3 [114](#), [151](#), [152](#)
Port Forwarding [269](#)
Power Specification [267](#)
PPP (Point-to-Point Protocol) Link Layer Protocol [268](#)

PPP over ATM AAL5 [268](#)
PPP over Ethernet [268](#)
PPPoE [81](#)
 Benefits [81](#)
PPPoE (Point-to-Point Protocol over Ethernet) [38](#), [81](#)
PPTP [114](#)
Priorities [191](#)
Priority [193](#)
Priority-based Scheduler [188](#)
PSTN (Public Switched Telephone Network) [35](#)
PSTN Call Setup Signaling [126](#)
Pulse Code Modulation [125](#)
Pulse Dialing [126](#)
PVCs [268](#)

Q

QoS [131](#)
QoS (Quality of Service) [38](#)
Quality of Service [131](#)
Quality of Service, See QoS
Quick Dialing [269](#)
Quick Start Guide [33](#), [45](#)

R

Reach-Extended ADSL [268](#)
Real Time E-mail Alerts [268](#)
Real Time Transport Protocol [125](#)
reinitialize the ADSL line [251](#)
Related Documentation [33](#)
Remote Management and NAT [202](#)
Remote Management Limitations [201](#)
Reports and Logs [268](#)
Reset Button [47](#)
Resetting Your Device [47](#)
Restore [239](#)
Restore Configuration [244](#)
RFC 1483 [82](#), [268](#)
RFC 1631 [109](#)
RFC 1889 [125](#), [269](#)
RFC 1890 [269](#)
RFC 2327 [269](#)
RFC 2364 [268](#)
RFC 2516 [38](#), [268](#)
RFC 2684 [268](#)

RFC 3261 [269](#)
 RIP, See Routing Information Protocol [98](#)
 Romfile [235](#)
 Router [34](#)
 Routing Information Protocol [98](#)
 Direction [98](#)
 Version [98](#)
 RTCP [269](#)
 RTP [269](#)
 RTP (Real Time Transport Protocol) [125](#)
 Rules [164](#)
 Checklist [162](#)
 Key Fields [163](#)
 LAN to WAN [164](#)
 Logic [162](#)

S

Safety Warnings [6](#)
 Saving the State [155](#)
 Scheduler [188](#)
 SDP [269](#)
 Seamless Rate Adaptation [268](#)
 Security In General [158](#)
 Security Ramifications [162](#)
 Server [34](#), [226](#)
 Service [163](#)
 Service Type [171](#), [254](#)
 Services [114](#)
 Services, common [114](#)
 Session Description Protocol [269](#)
 Session Initiating Protocol [269](#)
 Session Initiation Protocol [119](#)
 Silence Suppression [38](#), [133](#), [269](#)
 Single User Account (SUA) [40](#)
 SIP [119](#)
 Account [119](#)
 Accounts [38](#)
 Call Progression [120](#)
 Call Progression, ACK Message [120](#)
 Call Progression, BYE Request [120](#)
 Call Progression, OK Response [120](#)
 Call Progression, SIP INVITE Request [120](#)
 Client [120](#)
 Identities [119](#)
 Multiple [38](#)
 Number [119](#)
 Proxy Server [121](#)
 Redirect Server [122](#)
 Register Server [123](#)
 Servers [120](#)
 Service Domain [120](#)
 URI [119](#)
 User Agent [121](#)
 SIP ALG [38](#), [117](#)
 SIP ALG Passthrough [268](#)
 SIP Application Layer Gateway [38](#), [117](#)
 SIP Number [63](#)
 SIP Server Address [63](#)
 SIP Service Domain [64](#)
 SIP Version 2 [269](#)
 SIP, Authentication Password [64](#)
 SIP, Authentication User ID [64](#)
 SMTP [114](#)
 SMTP Error Messages [233](#)
 Smurf [154](#)
 Smurf, attack [153](#)
 SNMP [114](#), [205](#), [268](#)
 Manager [206](#)
 MIBs [207](#)
 SOHO (Small Office/Home Office) [40](#)
 Source Address [163](#)
 Speed Dial [141](#), [147](#)
 Splitters [271](#)
 SRA [268](#)
 Stateful Inspection [37](#), [149](#), [150](#), [155](#)
 on Your ZyXEL Device [156](#)
 Process [156](#)
 Stateful Packet Inspection [268](#)
 Static Route [183](#)
 Storage Humidity [267](#)
 Storage Temperature [267](#)
 SUA [112](#)
 SUA (Single User Account) [112](#)
 SUA vs NAT [112](#)
 Subnet Mask [97](#), [169](#)
 Subnet Masks [286](#)
 Subnetting [286](#)
 Supplementary Phone Services [137](#)
 Supplementary Services [137](#)
 Supporting Disk [33](#)
 Sustain Cell Rate (SCR) [90](#)
 Sustained Cell Rate (SCR) [84](#)
 Switch [34](#)
 SYN Flood [152](#), [153](#)
 SYN-ACK [153](#)
 Syntax Conventions [33](#)
 Syslog [174](#)
 System Name [224](#)
 System Parameter Table Generator [317](#)
 System Timeout [202](#)

T

TCP Maximum Incomplete [176, 177](#)
TCP Security [157](#)
TCP/IP [151, 152](#)
Teardrop [152](#)
Telephone [34](#)
Telnet [203](#)
Temperature [267](#)
Text File Format [317](#)
TFTP
 File Upload [246](#)
TFTP and FTP over WAN [236](#)
TFTP Restrictions [201, 236](#)
Three-Way Conference [139, 140](#)
Three-Way Handshake [152](#)
Threshold Values [175](#)
ToS [131](#)
Traceroute [155](#)
Traffic Redirect [91, 92, 93, 94](#)
Traffic shaping [84](#)
Transparent Bridging [268](#)
Triangle [299](#)
Triangle Route Solutions [300](#)
Type Of Service [131](#)

U

UBR (Unspecified Bit Rate) [90](#)
UDP/ICMP Security [157](#)
Uniform Resource Identifier [119](#)
Universal Plug and Play [211](#)
 Application [211](#)
 Security issues [212](#)
Universal Plug and Play (UPnP) [38](#)
Universal Plug and Play Forum [212](#)
Upload Firmware [245](#)
UPnP [211](#)
Upper Layer Protocols [157, 158](#)
USA Type Call Service Mode [139](#)
User Name [198](#)
Using Speed Dial [147](#)

V

VAD [133, 269](#)

VAD (Voice Activity Detection) [38](#)
VBR-nRT [90](#)
VBR-RT [90](#)
Virtual Channel Identifier (VCI) [82](#)
virtual circuit (VC) [82](#)
Virtual Local Area Network [132](#)
Virtual Path Identifier (VPI) [82](#)
VLAN [132](#)
VLAN Group [132](#)
VLAN ID [132](#)
VLAN ID Tags [132](#)
Voice Activity Detection [133, 269](#)
Voice Channels [38](#)
Voice Channels, Multiple [38](#)
Voice Coding [125](#)
VoIP [119](#)
VoIP Standards Compliance [38](#)
VPI & VCI [82](#)
VPN (Virtual Private Network) [35](#)

W

WAN (Wide Area Network) [81](#)
WAN to LAN Rules [164](#)
Warranty [7](#)
Web [202](#)
Web Configurator [45, 158, 163](#)

Z

Zero Configuration Internet Access [37, 86](#)
ZyNOS [236](#)
ZyNOS (ZyXEL Network Operating System) [235](#)
ZyNOS F/W Version [236](#)
ZyXEL Home Page [4](#)