

P-2602HWNLI

802.11g Wireless ADSL2+ 4-Port VoIP IAD

User's Guide

Version 3.40

5/2006

Edition 1

ZyXEL

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

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

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

Notice 1

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

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

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

Viewing Certifications

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



Safety Warnings

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

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Connect the power cord to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

ZyXEL Limited Warranty

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

Note

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

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

Customer Support

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

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

METHOD LOCATION	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
	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 Malminkari 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, Zoldiomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		

LOCATION	METHOD	SUPPORT E-MAIL	TELEPHONE^A	WEB SITE	REGULAR MAIL
		SALES E-MAIL	FAX	FTP SITE	
POLAND		info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzesi 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 5 ^a 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	25
List of Tables	31
Preface	37
Chapter 1	
Getting To Know the ZyXEL Device.....	39
1.1 Introducing the ZyXEL Device	39
1.2 Features	40
1.3 Applications	46
1.3.1 Internet Access	46
1.3.1.1 Internet Single User Account	46
1.3.2 Making Calls via Internet Telephony Service Provider	46
1.3.3 Make Peer-to-peer Calls	47
1.3.4 Firewall for Secure Broadband Internet Access	47
1.3.5 LAN to LAN Application	48
1.3.6 Lights	49
1.4 Splitters and Microfilters	50
1.4.1 Connecting a POTS Splitter	51
1.4.2 Telephone Microfilters	51
Chapter 2	
Introducing the Web Configurator.....	53
2.1 Web Configurator Overview	53
2.1.1 Accessing the Web Configurator	53
2.1.2 The RESET Button	55
2.1.2.1 Using The Reset Button	55
2.2 Web Configurator Main Screen	56

2.2.1 Title Bar	56
2.2.2 Navigation Panel	57
2.2.3 Main Window	59
2.2.4 Status Bar	59
Chapter 3	
Internet and Wireless Setup Wizard	61
3.1 Introduction	61
3.2 Internet Access Wizard Setup	61
3.2.1 Manual Configuration	63
3.3 Wireless Connection Wizard Setup	69
3.3.1 Manually Assign a WPA key	73
3.3.2 Manually Assign a WEP key	73
Chapter 4	
VoIP Wizard	77
4.1 Introduction	77
4.2 VOIP Wizard Setup	77
Chapter 5	
Bandwidth Management Wizard	81
5.1 Introduction	81
5.2 Predefined Media Bandwidth Management Services	81
5.3 Bandwidth Management Wizard Setup	82
Chapter 6	
WAN Setup	87
6.1 WAN Overview	87
6.1.1 Encapsulation	87
6.1.1.1 ENET ENCAP	87
6.1.1.2 PPP over Ethernet	87
6.1.1.3 PPPoA	87
6.1.1.4 RFC 1483	88
6.1.2 Multiplexing	88
6.1.2.1 VC-based Multiplexing	88
6.1.2.2 LLC-based Multiplexing	88
6.1.3 VPI and VCI	88
6.1.4 IP Address Assignment	88
6.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation	88
6.1.4.2 IP Assignment with RFC 1483 Encapsulation	89
6.1.4.3 IP Assignment with ENET ENCAP Encapsulation	89
6.1.5 Nailed-Up Connection (PPP)	89
6.2 PPPoE Encapsulation	89

6.3 Metric	90
6.4 Traffic Shaping	90
6.4.1 ATM Traffic Classes	91
6.4.1.1 Constant Bit Rate (CBR)	91
6.4.1.2 Variable Bit Rate (VBR)	91
6.4.1.3 Unspecified Bit Rate (UBR)	92
6.5 Zero Configuration Internet Access	92
6.6 Internet Access Setup	92
6.6.1 Advanced Internet Access Setup	95
6.7 Configuring More Connections	96
6.8 More Connections Edit	97
6.9 More Connections Edit Advanced	99
6.10 Configuring WAN Backup	100
Chapter 7	
Status Screens	103
7.1 Status Screen	103
7.2 Client List	107
7.3 Any IP Table	109
7.4 WLAN Status	109
7.4.1 Bandwidth Status	110
7.4.2 VPN Status	111
7.5 Packet Statistics	112
7.6 VoIP Statistics	114
Chapter 8	
LAN Setup	117
8.1 LAN Overview	117
8.1.1 LANs, WANs and the ZyXEL Device	117
8.1.2 DHCP Setup	118
8.1.2.1 IP Pool Setup	118
8.1.3 DNS Server Address	118
8.1.4 DNS Server Address Assignment	119
8.2 LAN TCP/IP	119
8.2.1 IP Address and Subnet Mask	119
8.2.1.1 Private IP Addresses	120
8.2.2 RIP Setup	120
8.2.3 Multicast	121
8.2.4 Any IP	121
8.2.4.1 How Any IP Works	122
8.3 Configuring LAN IP	123
8.3.1 Configuring Advanced LAN Setup	123
8.4 DHCP Setup	125

8.5 LAN Client List	126
8.6 LAN IP Alias	128
Chapter 9	
Wireless LAN	131
9.1 Wireless Network Overview	131
9.2 Wireless Security Overview	131
9.2.1 SSID	131
9.2.2 MAC Address Filter	132
9.2.3 User Authentication	132
9.2.4 Encryption	132
9.2.5 One-Touch Intelligent Security Technology (OTIST)	133
9.3 Wireless Performance Overview	134
9.3.1 Quality of Service (QoS)	134
9.4 General Wireless LAN Screen	134
9.4.1 WEP Encryption	135
9.4.2 WPA-PSK/WPA2-PSK	136
9.4.3 WPA/WPA2	138
9.4.4 Wireless LAN Advanced Setup	140
9.5 OTIST	142
9.5.1 Enabling OTIST	142
9.5.1.1 AP	142
9.5.1.2 Wireless Client	143
9.5.2 Starting OTIST	144
9.5.3 Notes on OTIST	145
9.6 MAC Filter	145
9.7 WMM QoS	147
9.7.1 WMM QoS Example	147
9.7.2 WMM QoS Priorities	147
9.7.3 Services	148
9.8 QoS Screen	148
9.8.1 ToS (Type of Service) and WMM QoS	148
9.8.2 Application Priority Configuration	150
Chapter 10	
Network Address Translation (NAT) Screens	153
10.1 NAT Overview	153
10.1.1 NAT Definitions	153
10.1.2 What NAT Does	154
10.1.3 How NAT Works	154
10.1.4 NAT Application	155
10.1.5 NAT Mapping Types	155
10.2 SUA (Single User Account) Versus NAT	156

10.3 NAT General Setup	157
10.4 Port Forwarding	158
10.4.1 Default Server IP Address	158
10.4.2 Port Forwarding: Services and Port Numbers	158
10.4.3 Configuring Servers Behind Port Forwarding (Example)	158
10.5 Configuring Port Forwarding	159
10.5.1 Port Forwarding Rule Edit	161
10.6 Address Mapping	161
10.6.1 Address Mapping Rule Edit	163
Chapter 11	
Voice	165
11.1 Introduction to VoIP	165
11.2 SIP	165
11.2.1 SIP Identities	165
11.2.1.1 SIP Number	165
11.2.1.2 SIP Service Domain	166
11.2.2 SIP Call Progression	166
11.2.3 SIP Servers	166
11.2.3.1 SIP User Agent	167
11.2.3.2 SIP Proxy Server	167
11.2.3.3 SIP Redirect Server	168
11.2.3.4 SIP Register Server	169
11.3 SIP Settings Screen	169
11.3.1 RTP	171
11.4 SIP ALG	171
11.5 Voice Coding	171
11.6 PSTN Call Setup Signaling	172
11.7 MWI (Message Waiting Indication)	172
11.8 Custom Tones (IVR)	172
11.8.0.1 Recording Custom Tones	172
11.8.0.2 Listening to Custom Tones	173
11.8.0.3 Deleting Custom Tones	173
11.9 Advanced SIP Setup Screen	173
11.10 Quality of Service (QoS)	177
11.10.1 Type Of Service (ToS)	177
11.10.2 VLAN	177
11.10.3 SIP QoS Screen	177
11.11 Phone	178
11.12 PSTN Line	178
11.13 ISDN Line	179
11.13.1 Voice Activity Detection/Silence Suppression	179
11.13.2 Comfort Noise Generation	179

11.13.3 Echo Cancellation	179
11.14 Analog Phone Screen	179
11.15 Advanced Analog Phone Setup Screen	181
11.16 ISDN Phone Screen	182
11.17 Common Phone Settings Screen	182
11.18 Supplementary Phone Services Overview (PSTN)	183
11.18.1 The Flash Key	184
11.18.2 Europe Type Supplementary Phone Services	184
11.18.2.1 European Call Hold	184
11.18.2.2 European Call Waiting	185
11.18.2.3 European Call Transfer	185
11.18.2.4 European Three-Way Conference	185
11.18.2.5 European Call Return	186
11.18.3 USA Type Supplementary Services	186
11.18.3.1 USA Call Hold	186
11.18.3.2 USA Call Waiting	186
11.18.3.3 USA Call Transfer	186
11.18.3.4 USA Three-Way Conference	187
11.18.3.5 USA Call Return	187
11.19 Supplementary Phone Services Overview (ISDN)	187
11.20 Phone Region Screen	188
11.21 Speed Dial	189
11.21.1 Peer-to-Peer Calls	189
11.22 Speed Dial Screen	190
11.23 Incoming Call Policy Screen	191
11.24 PSTN Line Screen	193
11.25 ISDN Line Screen	194
Chapter 12 Phone Usage	197
12.1 Dialing a Telephone Number	197
12.2 Using Speed Dial to Dial a Telephone Number	197
12.3 Internal Calls	197
12.4 Checking the Device's IP Address	197
12.5 Auto Firmware Upgrade	198
Chapter 13 Firewalls	199
13.1 Firewall Overview	199
13.2 Types of Firewalls	199
13.2.1 Packet Filtering Firewalls	199
13.2.2 Application-level Firewalls	200
13.2.3 Stateful Inspection Firewalls	200

13.3 Introduction to ZyXEL's Firewall	200
13.3.1 Denial of Service Attacks	201
13.4 Denial of Service	201
13.4.1 Basics	201
13.4.2 Types of DoS Attacks	202
13.4.2.1 ICMP Vulnerability	204
13.4.2.2 Illegal Commands (NetBIOS and SMTP)	204
13.4.2.3 Traceroute	205
13.5 Stateful Inspection	205
13.5.1 Stateful Inspection Process	206
13.5.2 Stateful Inspection on Your ZyXEL Device	207
13.5.3 TCP Security	207
13.5.4 UDP/ICMP Security	208
13.5.5 Upper Layer Protocols	208
13.6 Guidelines for Enhancing Security with Your Firewall	209
13.6.1 Security In General	209

Chapter 14

Firewall Configuration 211

14.1 Access Methods	211
14.2 Firewall Policies Overview	211
14.3 Rule Logic Overview	212
14.3.1 Rule Checklist	212
14.3.2 Security Ramifications	212
14.3.3 Key Fields For Configuring Rules	213
14.3.3.1 Action	213
14.3.3.2 Service	213
14.3.3.3 Source Address	213
14.3.3.4 Destination Address	213
14.4 Connection Direction	213
14.4.1 LAN to WAN Rules	214
14.4.2 Alerts	214
14.5 Triangle Route	214
14.5.1 The "Triangle Route" Problem	214
14.5.2 Solving the "Triangle Route" Problem	215
14.6 General Firewall Policy	216
14.7 Firewall Rules Summary	218
14.7.1 Configuring Firewall Rules	219
14.7.2 Customized Services	222
14.7.3 Configuring A Customized Service	223
14.8 Example Firewall Rule	223
14.9 Predefined Services	227
14.10 Firewall Threshold	227

14.10.1 Threshold Values	227
14.10.2 Half-Open Sessions	228
14.10.2.1 TCP Maximum Incomplete and Blocking Time	228
14.10.3 Configuring Firewall Thresholds	229
Chapter 15	
Content Filtering	231
15.1 Content Filtering Overview	231
15.2 Configuring Keyword Blocking	231
15.3 Configuring the Schedule	232
15.4 Configuring Trusted Computers	233
Chapter 16	
Introduction to IPSec	235
16.1 VPN Overview	235
16.1.1 IPSec	235
16.1.2 Security Association	235
16.1.3 Other Terminology	235
16.1.3.1 Encryption	235
16.1.3.2 Data Confidentiality	236
16.1.3.3 Data Integrity	236
16.1.3.4 Data Origin Authentication	236
16.1.4 VPN Applications	236
16.2 IPSec Architecture	237
16.2.1 IPSec Algorithms	237
16.2.2 Key Management	237
16.3 Encapsulation	237
16.3.1 Transport Mode	238
16.3.2 Tunnel Mode	238
16.4 IPSec and NAT	238
Chapter 17	
VPN Screens	241
17.1 VPN/IPSec Overview	241
17.2 IPSec Algorithms	241
17.2.1 AH (Authentication Header) Protocol	241
17.2.2 ESP (Encapsulating Security Payload) Protocol	241
17.3 My IP Address	242
17.4 Secure Gateway Address	243
17.4.1 Dynamic Secure Gateway Address	243
17.5 VPN Setup Screen	243
17.6 Keep Alive	245
17.7 VPN, NAT, and NAT Traversal	246

17.8 Remote DNS Server	247
17.9 ID Type and Content	247
17.9.1 ID Type and Content Examples	248
17.10 Pre-Shared Key	249
17.11 Editing VPN Policies	249
17.12 IKE Phases	254
17.12.1 Negotiation Mode	255
17.12.2 Diffie-Hellman (DH) Key Groups	256
17.12.3 Perfect Forward Secrecy (PFS)	256
17.13 Configuring Advanced IKE Settings	256
17.14 Manual Key Setup	259
17.14.1 Security Parameter Index (SPI)	259
17.15 Configuring Manual Key	259
17.16 Viewing SA Monitor	262
17.17 Configuring Global Setting	264
17.18 Telecommuter VPN/IPSec Examples	264
17.18.1 Telecommuters Sharing One VPN Rule Example	264
17.18.2 Telecommuters Using Unique VPN Rules Example	265
17.19 VPN and Remote Management	267
Chapter 18	
Static Route	269
18.1 Static Route	269
18.2 Configuring Static Route	269
18.2.1 Static Route Edit	271
Chapter 19	
Bandwidth Management	273
19.1 Bandwidth Management Overview	273
19.2 Application-based Bandwidth Management	273
19.3 Subnet-based Bandwidth Management	273
19.4 Application and Subnet-based Bandwidth Management	274
19.5 Scheduler	274
19.5.1 Priority-based Scheduler	274
19.5.2 Fairness-based Scheduler	274
19.6 Maximize Bandwidth Usage	275
19.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic	275
19.6.2 Maximize Bandwidth Usage Example	275
19.6.2.1 Priority-based Allotment of Unused and Unallocated Bandwidth	276
19.6.2.2 Fairness-based Allotment of Unused and Unallocated Bandwidth ...	276
19.6.3 Bandwidth Management Priorities	277
19.7 Over Allotment of Bandwidth	277

19.8 Configuring Summary	278
19.9 Bandwidth Management Rule Setup	279
19.9.1 Rule Configuration	280
19.10 Bandwidth Monitor	283
Chapter 20	
Dynamic DNS Setup.....	285
20.1 Dynamic DNS Overview	285
20.1.1 DYNDNS Wildcard	285
20.2 Configuring Dynamic DNS	285
Chapter 21	
Remote Management Configuration	289
21.1 Remote Management Overview	289
21.1.1 Remote Management Limitations	289
21.1.2 Remote Management and NAT	290
21.1.3 System Timeout	290
21.2 WWW	290
21.3 Telnet	291
21.4 Configuring Telnet	292
21.5 Configuring FTP	293
21.6 SNMP	294
21.6.1 Supported MIBs	295
21.6.2 SNMP Traps	295
21.6.3 Configuring SNMP	296
21.7 Configuring DNS	297
21.8 Configuring ICMP	298
Chapter 22	
Universal Plug-and-Play (UPnP)	301
22.1 Introducing Universal Plug and Play	301
22.1.1 How do I know if I'm using UPnP?	301
22.1.2 NAT Traversal	301
22.1.3 Cautions with UPnP	302
22.2 UPnP and ZyXEL	302
22.2.1 Configuring UPnP	302
22.3 Installing UPnP in Windows Example	303
22.4 Using UPnP in Windows XP Example	307
Chapter 23	
System	313
23.1 General Setup and System Name	313
23.1.1 General Setup	313

23.2 Time Setting	315
Chapter 24	
Logs	319
24.1 Logs Overview	319
24.1.1 Alerts and Logs	319
24.2 Viewing the Logs	319
24.3 Configuring Log Settings	320
24.4 SMTP Error Messages	323
24.4.1 Example E-mail Log	323
24.5 Log Descriptions	324
Chapter 25	
Tools	333
25.1 Introduction	333
25.2 Filename Conventions	333
25.3 File Maintenance Over WAN	334
25.4 Firmware Upgrade Screen	334
25.5 Backup and Restore	336
25.5.1 Backup Configuration	337
25.5.2 Restore Configuration	338
25.5.3 Reset to Factory Defaults	339
25.6 Restart	340
25.7 Using FTP or TFTP to Back Up Configuration	340
25.7.1 Using the FTP Commands to Back Up Configuration	340
25.7.2 FTP Command Configuration Backup Example	340
25.7.3 Configuration Backup Using GUI-based FTP Clients	341
25.7.4 Backup Configuration Using TFTP	341
25.7.5 TFTP Command Configuration Backup Example	342
25.7.6 Configuration Backup Using GUI-based TFTP Clients	342
25.8 Using FTP or TFTP to Restore Configuration	343
25.8.1 Restore Using FTP Session Example	343
25.9 FTP and TFTP Firmware and Configuration File Uploads	343
25.9.1 FTP File Upload Command from the DOS Prompt Example	343
25.9.2 FTP Session Example of Firmware File Upload	344
25.9.3 TFTP File Upload	344
25.9.4 TFTP Upload Command Example	345
Chapter 26	
Diagnostic	347
26.1 General Diagnostic	347
26.2 DSL Line Diagnostic	347

Chapter 27	
Troubleshooting	351
27.1 Problems Starting Up the ZyXEL Device	351
27.2 Problems with the LAN	351
27.3 Problems with the WAN	352
27.4 Problems Accessing the ZyXEL Device	353
27.4.1 Pop-up Windows, JavaScripts and Java Permissions	353
27.4.1.1 Internet Explorer Pop-up Blockers	354
27.4.1.2 JavaScripts	357
27.4.1.3 Java Permissions	359
27.5 Telephone Problems	361
Appendix A	
Product Specifications	363
Power Adapter Specifications	366
Appendix B	
Setting up Your Computer's IP Address.....	369
Windows 95/98/Me.....	369
Configuring	371
Verifying Settings	372
Windows 2000/NT/XP.....	372
Verifying Settings	376
Macintosh OS 8/9.....	376
Verifying Settings	378
Macintosh OS X	378
Verifying Settings	379
Appendix C	
IP Subnetting	381
IP Addressing	381
IP Classes	381
Subnet Masks	382
Subnetting	382
Example: Two Subnets	383
Example: Four Subnets.....	385
Example Eight Subnets.....	386
Subnetting With Class A and Class B Networks.....	387
Appendix D	
About ADSL	389
Introduction to DSL	389

ADSL Overview.....	389
Advantages of ADSL.....	389
Appendix E Virtual Circuit Topology	391
Appendix F Wireless LANs	393
Wireless LAN Topologies	393
Ad-hoc Wireless LAN Configuration	393
BSS.....	393
ESS.....	394
Channel.....	395
RTS/CTS	395
Fragmentation Threshold	396
Preamble Type	397
IEEE 802.11g Wireless LAN	397
Wireless Security Overview	398
IEEE 802.1x	398
RADIUS.....	399
Types of RADIUS Messages	399
Types of Authentication.....	400
EAP-MD5 (Message-Digest Algorithm 5)	400
EAP-TLS (Transport Layer Security)	400
EAP-TTLS (Tunneled Transport Layer Service)	400
PEAP (Protected EAP)	401
LEAP.....	401
Dynamic WEP Key Exchange.....	401
WPA and WPA2	402
Encryption	402
User Authentication	403
Wireless Client WPA Suplicants	403
WPA(2) with RADIUS Application Example	403
27.5.1 WPA(2)-PSK Application Example	404
Security Parameters Summary	405
Appendix G Common Services	407
Appendix H Internal SPTGEN	411
Internal SPTGEN Overview	411
The Configuration Text File Format.....	411

Internal SPTGEN File Modification - Important Points to Remember	412
Internal SPTGEN FTP Download Example.....	412
Internal SPTGEN FTP Upload Example	413
Example Internal SPTGEN Menus.....	414
Command Examples.....	426
Appendix I Commands.....	427
Accessing the Command Interpreter.....	427
Command Syntax.....	427
Command Usage	427
Filtering	427
The Filter Structure of the ZyXEL Device	429
Packet Filtering Vs. Firewall	430
Filter Commands	431
WAN Call Schedules.....	432
Index.....	435

List of Figures

Figure 1 Internet Access Application	46
Figure 2 Internet Telephony Service Provider Application	47
Figure 3 Peer-to-peer Calling	47
Figure 4 Firewall Application	48
Figure 5 LAN-to-LAN Application	49
Figure 6 Lights	49
Figure 7 Connecting a POTS Splitter	51
Figure 8 Connecting a Microfilter	52
Figure 9 Password Screen	54
Figure 10 Change Password Screen	54
Figure 11 Wizard or Advanced Screen	55
Figure 12 Main Screen	56
Figure 13 Select a Mode	61
Figure 14 Wizard Welcome	62
Figure 15 Auto Detection: No DSL Connection	62
Figure 16 Auto-Detection: PPPoE	63
Figure 17 Auto Detection: Failed	63
Figure 18 Internet Access Wizard Setup: ISP Parameters	64
Figure 19 Internet Connection with PPPoE	65
Figure 20 Internet Connection with RFC 1483	66
Figure 21 Internet Connection with ENET ENCAP	67
Figure 22 Internet Connection with PPPoA	68
Figure 23 Connection Test Failed-1	69
Figure 24 Connection Test Failed-2.	69
Figure 25 Connection Test Successful	70
Figure 26 Wireless LAN Setup Wizard 1	71
Figure 27 Wireless LAN	72
Figure 28 Manually Assign a WPA key	73
Figure 29 Manually Assign a WEP key	74
Figure 30 Wireless LAN Setup 3	75
Figure 31 Internet Access and WLAN Wizard Setup Complete	75
Figure 32 Select a Mode	77
Figure 33 Wizard: Welcome	78
Figure 34 VOIP Wizard Configuration	78
Figure 35 SIP Registration Test	79
Figure 36 VoIP Wizard Fail	79
Figure 37 VOIP Wizard Finish	80
Figure 38 Select a Mode	83

Figure 39 Wizard: Welcome	83
Figure 40 Bandwidth Management Wizard: General Information	84
Figure 41 Bandwidth Management Wizard: Service Configuration	85
Figure 42 Bandwidth Management Wizard: Complete	86
Figure 43 Example of Traffic Shaping	91
Figure 44 Internet Access Setup (PPPoE)	93
Figure 45 Advanced Internet Access Setup	95
Figure 46 More Connections	97
Figure 47 More Connections Edit	98
Figure 48 More Connections Edit Advanced	100
Figure 49 WAN Backup Setup	101
Figure 50 Status Screen	104
Figure 51 Client List	108
Figure 52 Any IP Table	109
Figure 53 WLAN Status	110
Figure 54 Bandwidth Status	111
Figure 55 Status: VPN Status	112
Figure 56 Packet Statistics	113
Figure 57 VoIP Statistics	114
Figure 58 LAN and WAN IP Addresses	117
Figure 59 Any IP Example	122
Figure 60 LAN IP	123
Figure 61 Advanced LAN Setup	124
Figure 62 DHCP Setup	125
Figure 63 LAN Client List	127
Figure 64 Physical Network & Partitioned Logical Networks	128
Figure 65 LAN IP Alias	129
Figure 66 Wireless LAN: General	134
Figure 67 Wireless: Static WEP Encryption	136
Figure 68 Wireless: WPA-PSK/WPA2-PSK	137
Figure 69 Wireless: WPA/WPA2	139
Figure 70 Advanced	141
Figure 71 OTIST	143
Figure 72 Example Wireless Client OTIST Screen	144
Figure 73 Security Key	144
Figure 74 OTIST in Progress (AP)	144
Figure 75 OTIST in Progress (Client)	144
Figure 76 No AP with OTIST Found	145
Figure 77 Start OTIST?	145
Figure 78 MAC Address Filter	146
Figure 79 Wireless LAN: QoS	149
Figure 80 Application Priority Configuration	150
Figure 81 How NAT Works	155

Figure 82 NAT Application With IP Alias	155
Figure 83 NAT General	157
Figure 84 Multiple Servers Behind NAT Example	159
Figure 85 Port Forwarding	160
Figure 86 Port Forwarding Rule Setup	161
Figure 87 Address Mapping Rules	162
Figure 88 Edit Address Mapping Rule	164
Figure 89 SIP User Agent	167
Figure 90 SIP Proxy Server	168
Figure 91 SIP Redirect Server	169
Figure 92 SIP > SIP Settings	170
Figure 93 VoIP > SIP Settings > Advanced	174
Figure 94 SIP > QoS	178
Figure 95 Phone > Analog Phone	180
Figure 96 Phone > Analog Phone > Advanced	181
Figure 97 Phone > ISDN Phone	182
Figure 98 Phone > Common	183
Figure 99 VoIP > Phone > Region	189
Figure 100 Phone Book > Speed Dial	190
Figure 101 Phone Book > Incoming Call Policy	192
Figure 102 PSTN Line > General	194
Figure 103 ISDN Line > General	195
Figure 104 Firewall Application	201
Figure 105 Three-Way Handshake	203
Figure 106 SYN Flood	203
Figure 107 Smurf Attack	204
Figure 108 Stateful Inspection	206
Figure 109 Ideal Firewall Setup	214
Figure 110 "Triangle Route" Problem	215
Figure 111 IP Alias	216
Figure 112 Firewall: General	217
Figure 113 Firewall Rules	218
Figure 114 Firewall: Edit Rule	220
Figure 115 Firewall: Customized Services	222
Figure 116 Firewall: Configure Customized Services	223
Figure 117 Firewall Example: Rules	224
Figure 118 Edit Custom Port Example	224
Figure 119 Firewall Example: Edit Rule: Destination Address	225
Figure 120 Firewall Example: Edit Rule: Select Customized Services	226
Figure 121 Firewall Example: Rules: MyService	227
Figure 122 Firewall: Threshold	229
Figure 123 Content Filter: Keyword	232
Figure 124 Content Filter: Schedule	233

Figure 125 Content Filter: Trusted	234
Figure 126 Encryption and Decryption	236
Figure 127 IPSec Architecture	237
Figure 128 Transport and Tunnel Mode IPSec Encapsulation	238
Figure 129 IPSec Summary Fields	243
Figure 130 VPN Setup	244
Figure 131 NAT Router Between IPSec Routers	246
Figure 132 VPN Host using Intranet DNS Server Example	247
Figure 133 Edit VPN Policies	250
Figure 134 Two Phases to Set Up the IPSec SA	254
Figure 135 Advanced VPN Policies	257
Figure 136 VPN: Manual Key	260
Figure 137 VPN: SA Monitor	263
Figure 138 VPN: Global Setting	264
Figure 139 Telecommuters Sharing One VPN Rule Example	265
Figure 140 Telecommuters Using Unique VPN Rules Example	266
Figure 141 Example of Static Routing Topology	269
Figure 142 Static Route	270
Figure 143 Static Route Edit	271
Figure 144 Subnet-based Bandwidth Management Example	274
Figure 145 Bandwidth Management: Summary	278
Figure 146 Bandwidth Management: Rule Setup	279
Figure 147 Bandwidth Management Rule Configuration	281
Figure 148 Bandwidth Management: Monitor	283
Figure 149 Dynamic DNS	286
Figure 150 Remote Management: WWW	291
Figure 151 Telnet Configuration on a TCP/IP Network	292
Figure 152 Remote Management: Telnet	292
Figure 153 Remote Management: FTP	293
Figure 154 SNMP Management Model	294
Figure 155 Remote Management: SNMP	296
Figure 156 Remote Management: DNS	298
Figure 157 Remote Management: ICMP	299
Figure 158 Configuring UPnP	303
Figure 159 Add/Remove Programs: Windows Setup: Communication	304
Figure 160 Add/Remove Programs: Windows Setup: Communication: Components 304	
Figure 161 Network Connections	305
Figure 162 Windows Optional Networking Components Wizard	306
Figure 163 Networking Services	306
Figure 164 Network Connections	307
Figure 165 Internet Connection Properties	308
Figure 166 Internet Connection Properties: Advanced Settings	309

Figure 167 Internet Connection Properties: Advanced Settings: Add	309
Figure 168 System Tray Icon	310
Figure 169 Internet Connection Status	310
Figure 170 Network Connections	311
Figure 171 Network Connections: My Network Places	312
Figure 172 Network Connections: My Network Places: Properties: Example	312
Figure 173 System General Setup	314
Figure 174 System Time Setting	315
Figure 175 View Log	320
Figure 176 Log Settings	321
Figure 177 E-mail Log Example	324
Figure 178 Firmware Upgrade	335
Figure 179 Firmware Upload In Progress	336
Figure 180 Network Temporarily Disconnected	336
Figure 181 Firmware Upload Error Message	336
Figure 182 Configuration	337
Figure 183 Configuration Upload Successful	338
Figure 184 Network Temporarily Disconnected	339
Figure 185 Configuration Upload Error	339
Figure 186 Reset Warning Message	339
Figure 187 Restart Screen	340
Figure 188 FTP Session Example	341
Figure 189 Restore Using FTP Session Example	343
Figure 190 FTP Session Example of Firmware File Upload	344
Figure 191 Diagnostic: General	347
Figure 192 Diagnostic: DSL Line	348
Figure 193 Pop-up Blocker	354
Figure 194 Internet Options	355
Figure 195 Internet Options	356
Figure 196 Pop-up Blocker Settings	357
Figure 197 Internet Options	358
Figure 198 Security Settings - Java Scripting	359
Figure 199 Security Settings - Java	360
Figure 200 Java (Sun)	361
Figure 201 Windows 95/98/Me: Network: Configuration	370
Figure 202 Windows 95/98/Me: TCP/IP Properties: IP Address	371
Figure 203 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	372
Figure 204 Windows XP: Start Menu	373
Figure 205 Windows XP: Control Panel	373
Figure 206 Windows XP: Control Panel: Network Connections: Properties	374
Figure 207 Windows XP: Local Area Connection Properties	374
Figure 208 Windows XP: Advanced TCP/IP Settings	375
Figure 209 Windows XP: Internet Protocol (TCP/IP) Properties	376

Figure 210 Macintosh OS 8/9: Apple Menu	377
Figure 211 Macintosh OS 8/9: TCP/IP	377
Figure 212 Macintosh OS X: Apple Menu	378
Figure 213 Macintosh OS X: Network	379
Figure 214 Virtual Circuit Topology	391
Figure 215 Peer-to-Peer Communication in an Ad-hoc Network	393
Figure 216 Basic Service Set	394
Figure 217 Infrastructure WLAN	395
Figure 218 RTS/CTS	396
Figure 219 WPA(2) with RADIUS Application Example	404
Figure 220 WPA(2)-PSK Authentication	405
Figure 221 Configuration Text File Format: Column Descriptions	411
Figure 222 Invalid Parameter Entered: Command Line Example	412
Figure 223 Valid Parameter Entered: Command Line Example	412
Figure 224 Internal SPTGEN FTP Download Example	413
Figure 225 Internal SPTGEN FTP Upload Example	413
Figure 226 Outgoing Packet Filtering Process	428
Figure 227 Filter Rule Process	429

List of Tables

Table 1 Models Covered	39
Table 2 ADSL Standards	40
Table 3 IEEE 802.11g	45
Table 4 Lights	50
Table 5 Web Configurator Icons in the Title Bar	56
Table 6 Navigation Panel Summary	57
Table 7 Internet Access Wizard Setup: ISP Parameters	64
Table 8 Internet Connection with PPPoE	65
Table 9 Internet Connection with RFC 1483	66
Table 10 Internet Connection with ENET ENCAP	67
Table 11 Internet Connection with PPPoA	68
Table 12 Wireless LAN Setup Wizard 1	71
Table 13 Wireless LAN Setup Wizard 2	72
Table 14 Manually Assign a WPA key	73
Table 15 Manually Assign a WEP key	74
Table 16 VOIP Wizard Configuration	78
Table 17 Media Bandwidth Management Setup: Services	81
Table 18 Bandwidth Management Wizard: General Information	84
Table 19 Bandwidth Management Wizard: Service Configuration	85
Table 20 Internet Access Setup	93
Table 21 Advanced Internet Access Setup	95
Table 22 More Connections	97
Table 23 More Connections Edit	98
Table 24 More Connections Edit Advanced	100
Table 25 WAN Backup Setup	101
Table 26 Status Screen	104
Table 27 Client List	108
Table 28 Any IP Table	109
Table 29 WLAN Status	110
Table 30 Status: VPN Status	112
Table 31 Packet Statistics	113
Table 32 VoIP Statistics	114
Table 33 LAN IP	123
Table 34 Advanced LAN Setup	124
Table 35 DHCP Setup	125
Table 36 LAN Client List	127
Table 37 LAN IP Alias	129
Table 38 Types of Encryption for Each Type of Authentication	133

Table 39 Wireless LAN: General	135
Table 40 Wireless: Static WEP Encryption	136
Table 41 Wireless: WPA-PSK/WPA2-PSK	137
Table 42 Wireless: WPA/WPA2	139
Table 43 Wireless LAN: Advanced	141
Table 44 OTIST	143
Table 45 MAC Address Filter	146
Table 46 WMM QoS Priorities	147
Table 47 Wireless LAN: QoS	149
Table 48 Application Priority Configuration	150
Table 49 NAT Definitions	153
Table 50 NAT Mapping Types	156
Table 51 NAT General	157
Table 52 Port Forwarding	160
Table 53 Port Forwarding Rule Setup	161
Table 54 Address Mapping Rules	162
Table 55 Edit Address Mapping Rule	164
Table 56 SIP Call Progression	166
Table 57 SIP > SIP Settings	170
Table 58 Custom Tones Details	172
Table 59 VoIP > SIP Settings > Advanced	175
Table 60 SIP > QoS	178
Table 61 Phone > Analog Phone	180
Table 62 Phone > Analog Phone > Advanced	181
Table 63 Phone > ISDN Phone	182
Table 64 Phone > Common	183
Table 65 European Flash Key Commands	184
Table 66 USA Flash Key Commands	186
Table 67 VoIP > Phone > Region	189
Table 68 Phone Book > Speed Dial	190
Table 69 Phone Book > Incoming Call Policy	192
Table 70 PSTN Line > General	194
Table 71 ISDN Line > General	195
Table 72 Common IP Ports	202
Table 73 ICMP Commands That Trigger Alerts	204
Table 74 Legal NetBIOS Commands	204
Table 75 Legal SMTP Commands	205
Table 76 Firewall: General	217
Table 77 Firewall Rules	218
Table 78 Firewall: Edit Rule	221
Table 79 Customized Services	222
Table 80 Firewall: Configure Customized Services	223
Table 81 Firewall: Threshold	229

Table 82 Content Filter: Keyword	232
Table 83 Content Filter: Schedule	233
Table 84 Content Filter: Trusted	234
Table 85 VPN and NAT	239
Table 86 AH and ESP	242
Table 87 VPN Setup	244
Table 88 VPN and NAT	246
Table 89 Local ID Type and Content Fields	248
Table 90 Peer ID Type and Content Fields	248
Table 91 Matching ID Type and Content Configuration Example	249
Table 92 Mismatching ID Type and Content Configuration Example	249
Table 93 Edit VPN Policies	250
Table 94 Advanced VPN Policies	257
Table 95 VPN: Manual Key	260
Table 96 VPN: SA Monitor	263
Table 97 VPN: Global Setting	264
Table 98 Telecommuters Sharing One VPN Rule Example	265
Table 99 Telecommuters Using Unique VPN Rules Example	266
Table 100 Static Route	270
Table 101 Static Route Edit	271
Table 102 Application and Subnet-based Bandwidth Management Example	274
Table 103 Maximize Bandwidth Usage Example	275
Table 104 Priority-based Allotment of Unused and Unallocated Bandwidth Example	276
Table 105 Fairness-based Allotment of Unused and Unallocated Bandwidth Example	276
Table 106 Bandwidth Management Priorities	277
Table 107 Over Allotment of Bandwidth Example	277
Table 108 Media Bandwidth Management: Summary	278
Table 109 Bandwidth Management: Rule Setup	279
Table 110 Bandwidth Management Rule Configuration	281
Table 111 Dynamic DNS	286
Table 112 Remote Management: WWW	291
Table 113 Remote Management: Telnet	292
Table 114 Remote Management: FTP	293
Table 115 SNMP Traps	295
Table 116 Remote Management: SNMP	296
Table 117 Remote Management: DNS	298
Table 118 Remote Management: ICMP	299
Table 119 Configuring UPnP	303
Table 120 System General Setup	314
Table 121 System Time Setting	315
Table 122 View Log	320

Table 123 Log Settings	321
Table 124 SMTP Error Messages	323
Table 125 System Maintenance Logs	324
Table 126 System Error Logs	325
Table 127 Access Control Logs	325
Table 128 TCP Reset Logs	326
Table 129 Packet Filter Logs	326
Table 130 ICMP Logs	327
Table 131 CDR Logs	327
Table 132 PPP Logs	327
Table 133 UPnP Logs	328
Table 134 Content Filtering Logs	328
Table 135 Attack Logs	328
Table 136 802.1X Logs	329
Table 137 ACL Setting Notes	330
Table 138 ICMP Notes	330
Table 139 Syslog Logs	331
Table 140 SIP Logs	331
Table 141 RTP Logs	332
Table 142 FSM Logs: Caller Side	332
Table 143 FSM Logs: Callee Side	332
Table 144 Filename Conventions	334
Table 145 Firmware Upgrade	335
Table 146 Restore Configuration	338
Table 147 General Commands for GUI-based FTP Clients	341
Table 148 General Commands for GUI-based TFTP Clients	342
Table 149 Diagnostic: General	347
Table 150 Diagnostic: DSL Line	349
Table 151 Troubleshooting Starting Up Your Device	351
Table 152 Troubleshooting the LAN	351
Table 153 Troubleshooting the WAN	352
Table 154 Troubleshooting Accessing Your Device	353
Table 155 Troubleshooting Telephone	361
Table 156 Device Specifications	363
Table 157 Firmware Specifications	364
Table 158 Power Adapter Specifications	366
Table 159 Classes of IP Addresses	381
Table 160 Allowed IP Address Range By Class	382
Table 161 “Natural” Masks	382
Table 162 Alternative Subnet Mask Notation	383
Table 163 Two Subnets Example	383
Table 164 Subnet 1	384
Table 165 Subnet 2	384

Table 166 Subnet 1	385
Table 167 Subnet 2	385
Table 168 Subnet 3	385
Table 169 Subnet 4	386
Table 170 Eight Subnets	386
Table 171 Class C Subnet Planning	386
Table 172 Class B Subnet Planning	387
Table 173 IEEE 802.11g	397
Table 174 Wireless Security Levels	398
Table 175 Comparison of EAP Authentication Types	401
Table 176 Wireless Security Relational Matrix	405
Table 177 Commonly Used Services	407
Table 178 Abbreviations Used in the Example Internal SPTGEN Screens Table ..	414
Table 179 Menu 1 General Setup	414
Table 180 Menu 3	414
Table 181 Menu 4 Internet Access Setup	418
Table 182 Menu 12	419
Table 183 Menu 15 SUA Server Setup	420
Table 184 Menu 21.1 Filter Set #1	421
Table 185 Menu 21.1 Filer Set #2,	423
Table 186 Menu 23 System Menus	424
Table 187 Menu 24.11 Remote Management Control	425
Table 188 Command Examples	426
Table 189 Filter Commands	431
Table 190 WAN Call Schedules	432

Preface

Congratulations on your purchase of the P-2602HWNLI 802.11g Wireless ADSL2+ 4-Port 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.

- ZyXEL Glossary and Web Site

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

User Guide Feedback

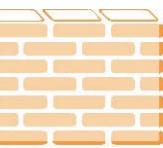
Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

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-2602HWNLI 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 ZyXEL Device

The ZyXEL Device is an Integrated Access Device (IAD) that combines an ADSL2+ router with Voice over IP (VoIP) communication capabilities to allow you to use a traditional analog or ISDN telephone to make Internet calls. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The ZyXEL Device 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-2602HWNLI-D3A
P-2602HWNLI-D7A

Please refer to the following description of the product name format.

- In the ZyXEL Device product name, “H” denotes an integrated 4-port switch (hub).
- “W” denotes wireless functionality. There is an embedded mini-PCI module for IEEE 802.11g wireless LAN connectivity.
- “N” denotes the ability to connect an ISDN (Integrated Services Digital Network) telephone to the device.
- “L” denotes the PSTN (Public Switched Telephone Network) line feature.

Note: When the ZyXEL Device does not have power, only the phone connected to the **PHONE 1** 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.

- “I” denotes the ISDN (Integrated Services Digital Network) line feature.¹

The P-2602HWNLI-D3A works over ISDN (Integrated Services Digital Network).

1. A device that includes both “L” and “I” in the model name can support either a PSTN line or a ISDN line, but not both at the same time.

The P-2602HWNLI-D7A 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 Ports

The 10/100 Mbps auto-negotiating Ethernet ports allow the device to detect the speed of incoming transmissions and adjust appropriately without manual intervention. Data transfer rates are either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.

The ports are auto-crossover (MDI/MDI-X) meaning they automatically adjust to either crossover or straight-through Ethernet cables.

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 following 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

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 1** 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.

ISDN Line

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

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.

Any IP

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

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.

4-port Switch

A combination of switch and router makes your ZyXEL Device a cost-effective and viable network solution. You can connect up to four computers to the ZyXEL Device without the cost of a hub. Use a hub to add more than four computers to your LAN.

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.

REN

A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.

Virtual Private Networks (VPN)

The ZyXEL Device allows companies to establish VPN connections with business partners, as well as with remote and branch offices. VPN uses data encryption and the Internet to provide transparent, secure communications between two or more sites without the expense of leased site-to-site lines. Moreover, using VPN, telecommuters and home workers can access data more easily and safely at home.

The ZyXEL Device VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

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. 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.

IEEE 802.11g Wireless LAN

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

Table 3 IEEE 802.11g

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

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

IEEE 802.11g+ Wireless LAN

Your device supports IEEE 802.11g+ to allow any ZyXEL WLAN devices that also support IEEE 802.1g+ to associate with the ZyXEL Device at higher transmission speeds than with standard IEEE 802.11g.

External Antenna

The ZyXEL Device is equipped with an attached antenna to provide a clear radio signal between the wireless stations and the access points.

Wireless LAN MAC Address Filtering

Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.

WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.

WPA2

WPA 2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services.

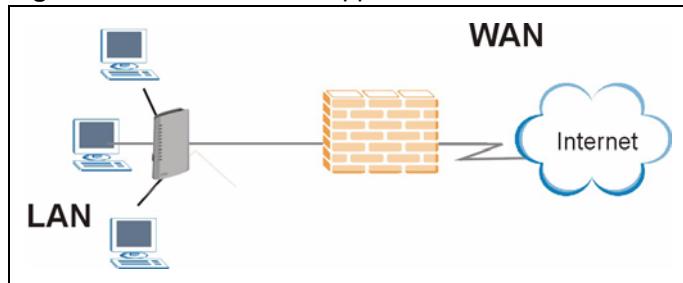
1.3 Applications

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

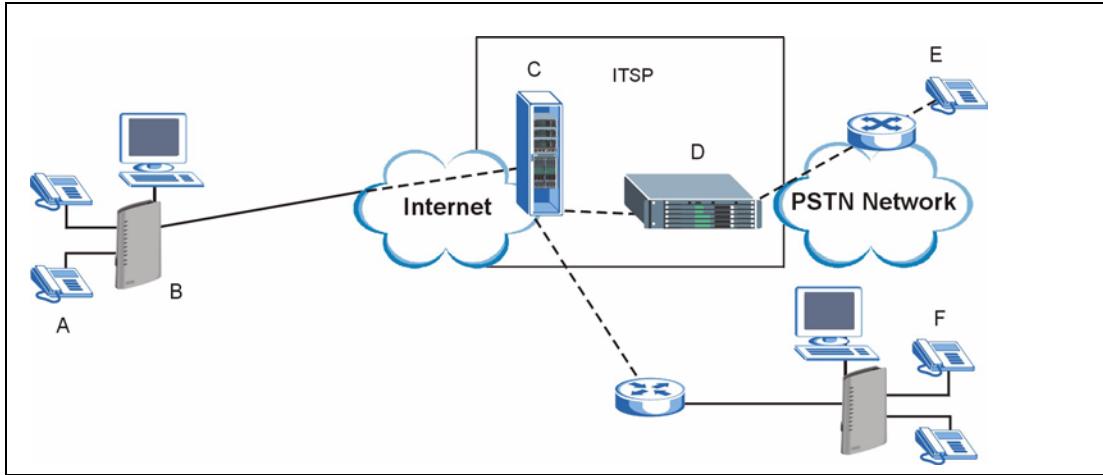
For a SOHO (Small Office/Home Office) environment, your device offers the Single User Account (SUA) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single IP address

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

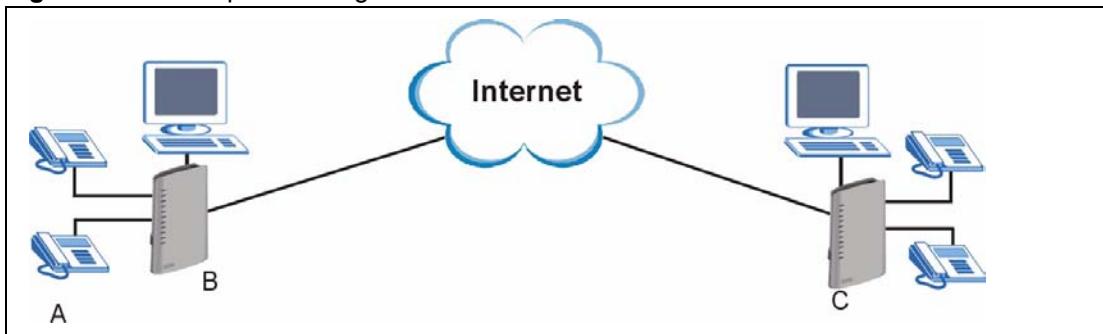


1.3.3 Make Peer-to-peer Calls

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).

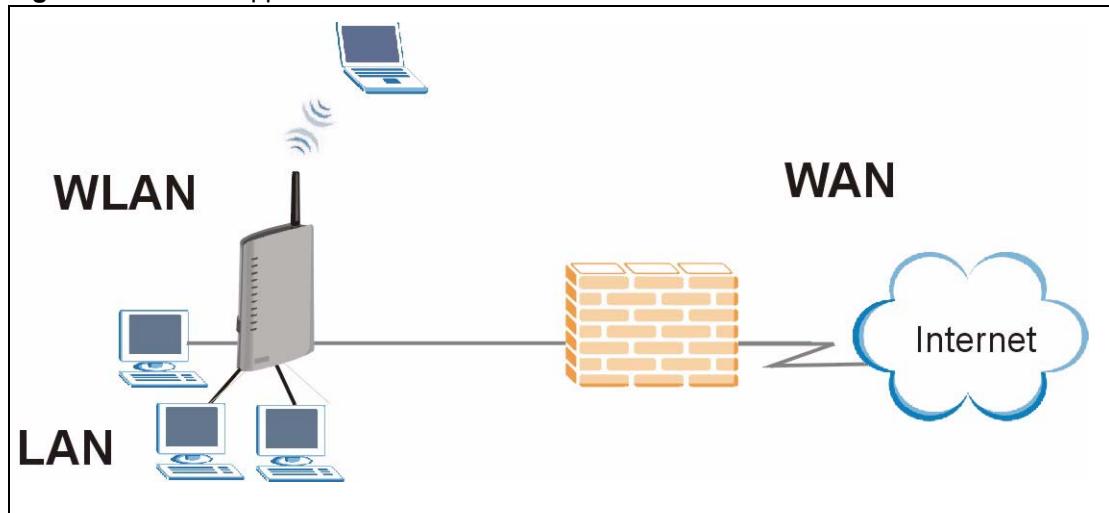
Figure 3 Peer-to-peer Calling



1.3.4 Firewall for Secure Broadband Internet Access

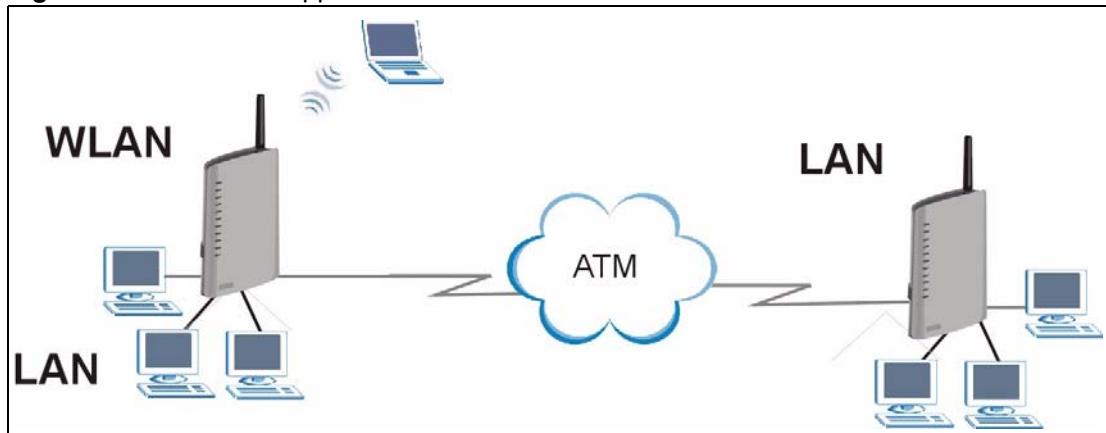
Your device provides protection from attacks by Internet hackers. By default, the firewall blocks all incoming traffic from the WAN. The firewall supports TCP/UDP inspection and DoS (Denial of Services) detection and prevention, as well as real time alerts, reports and logs.

Figure 4 Firewall Application

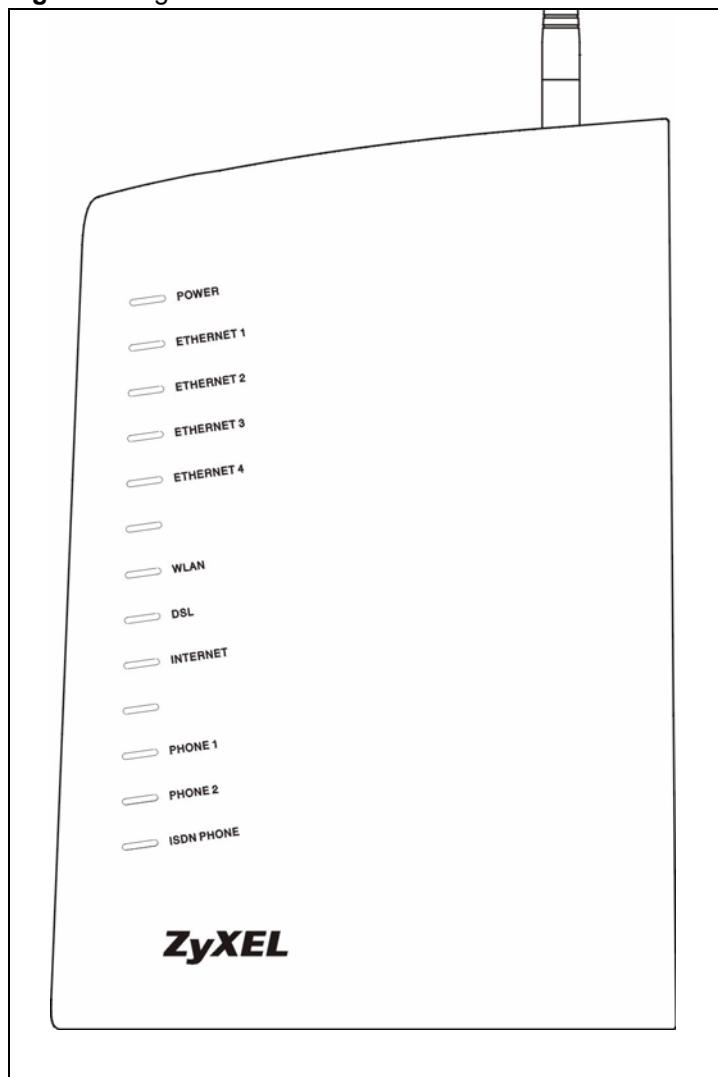


1.3.5 LAN to LAN Application

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

Figure 5 LAN-to-LAN Application

1.3.6 Lights

Figure 6 Lights

The following table describes your device's lights.

Table 4 Lights

LIGHT	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 1,2,3,4	Green	On	Your device has a successful Ethernet connection.
	Blinking		The ZyXEL Device is sending/receiving data.
	None	Off	The LAN is not connected.
WLAN	Green	On	Your device is ready, but is not sending/receiving data through the wireless LAN.
	Blinking		Your device is sending/receiving data through the wireless LAN.
	None	Off	The wireless LAN is not ready or has failed.
DSL	Green	On	Your device has a DSL connection.
	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.
	None	Off	The phone port does not have a SIP account registered.
ISDN PHONE	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.
	None	Off	The phone port does not have a SIP account registered.

1.4 Splitters and Microfilters

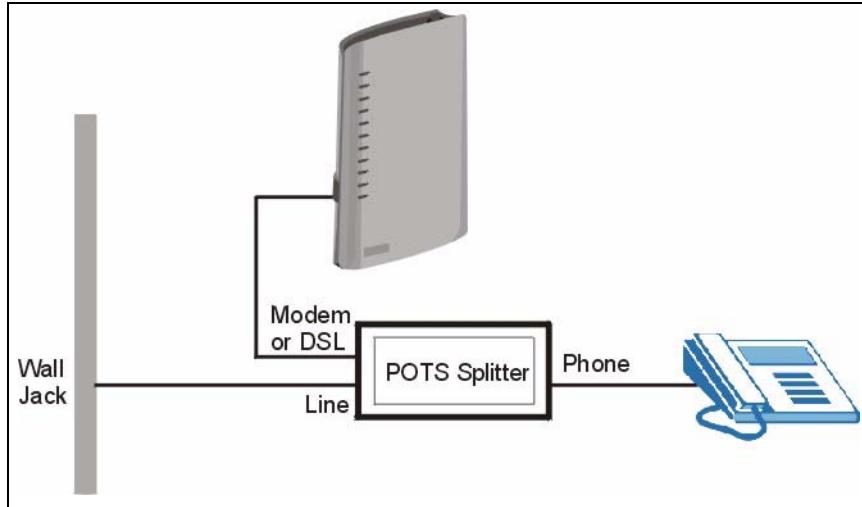
This section describes how to connect ADSL splitters and microfilters. See your Quick Start Guide for details on other hardware connections.

1.4.1 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 7 Connecting a POTS Splitter



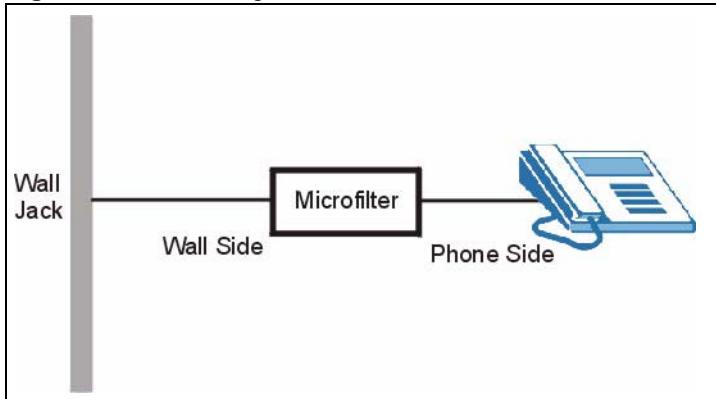
- 1 Connect the side labeled "Phone" to your telephone.
- 2 Connect the side labeled "Modem" or "DSL" to your ZyXEL Device.
- 3 Connect the side labeled "Line" to the telephone wall jack.

1.4.2 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 Locate and disconnect each telephone.
- 2 Connect a cable from the wall jack to the "wall side" of the microfilter.
- 3 Connect the "phone side" of the microfilter to your telephone as shown in the following figure.
- 4 After you are done, make sure that your telephone works. If your telephone does not work, disconnect the microfilter and contact either your local telephone company or the provider of the microfilter.

Figure 8 Connecting a Microfilter



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 the Troubleshooting chapter 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 9 Password Screen

- 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 10 Change Password Screen

- 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 61](#) 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 56](#) for more information.
 - Click **Exit** if you want to log out.

Note: For security reasons, by default 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 11 Wizard or Advanced Screen



2.1.2 The RESET Button

You can use the **RESET** button at the back of the device to turn the wireless LAN off or on. You can also use it to activate OTIST in order to assign your wireless security settings to wireless clients. 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** light is on (not blinking).

2 Do one of the following.

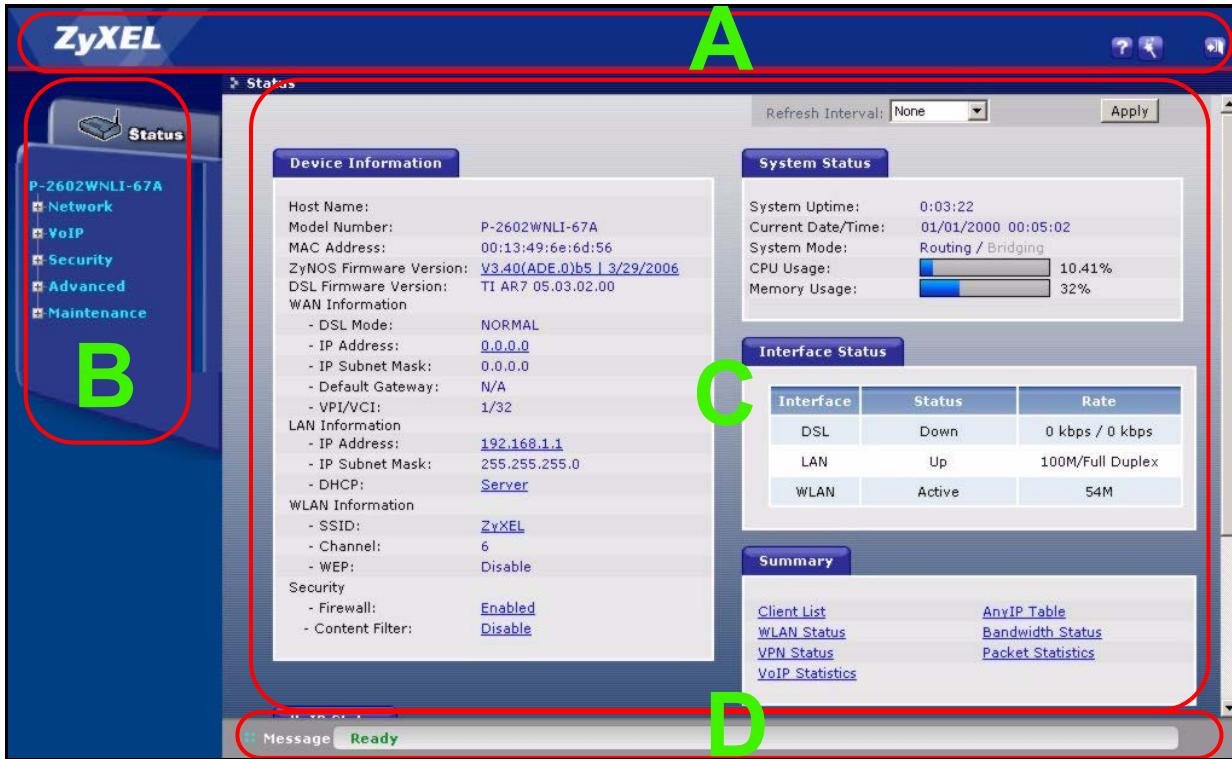
To turn the wireless LAN off or on, press the **RESET** button for one second and release it. The **WLAN** light should change from on to off or vice versa.

To activate OTIST in order to assign your wireless security settings to wireless clients, press the **RESET** button for five seconds and release it. The **WLAN** light should flash while the device uses OTIST to send wireless settings to OTIST clients.

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

2.2 Web Configurator Main Screen

Figure 12 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 provides some icons in the upper right corner.



The icons provide the following functions.

Table 5 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Wizards: Click this icon to go to the configuration wizards. See Chapter 3 on page 61 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 table describes the menu items.

Table 6 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 and place calls to a remote gateway.
	WAN Backup Setup	Use this screen to configure your traffic redirect properties and WAN backup settings.
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.
Wireless LAN	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	OTIST	Use this screen to assign your wireless security settings to wireless clients.
	MAC Filter	Use this screen to configure the ZyXEL Device to give exclusive access to specific wireless clients or exclude specific wireless clients from accessing the ZyXEL Device.
	QoS	WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Address Mapping	Use this screen to configure network address translation mapping rules.
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.
	ISDN Phone	Use this screen to set which SIP accounts the ISDN phone port uses.
	Common	Use this screen to configure general phone port settings.
	Region	Use this screen to select your location and call service mode.
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.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
PSTN Line	General	Use this screen to configure your ZyXEL Device's settings for PSTN calls.
ISDN Line	General	Use this screen to configure your ZyXEL Device's settings for ISDN 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.
	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.
VPN	Setup	Use this screen to configure each VPN tunnel.
	Monitor	Use this screen to look at the current status of each VPN tunnel.
	Global Settings	Use this screen to allow NetBIOS traffic through VPN tunnels.
Advanced		
Static Route	IP 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 bandwidth rules.
	Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Dynamic DNS	General	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		
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.

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
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 7 on page 103](#) 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 and Wireless Setup Wizard

This chapter provides information on the wizard setup screens for Internet access and wireless connections.

3.1 Introduction

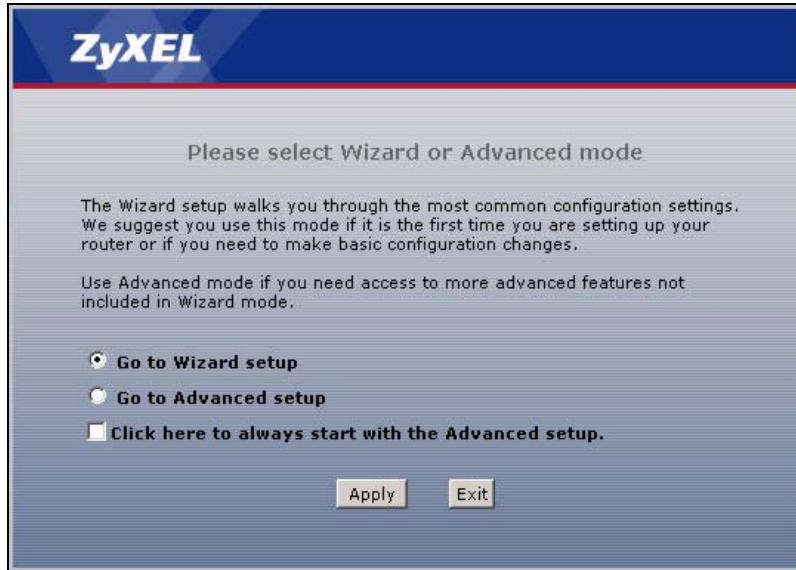
Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP. You also use them to configure your device for wireless connections.

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

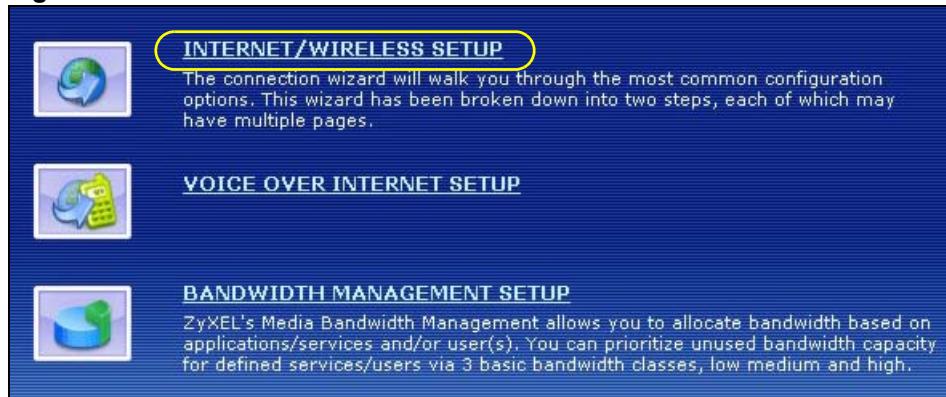
3.2 Internet Access Wizard Setup

- 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 13 Select a Mode



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

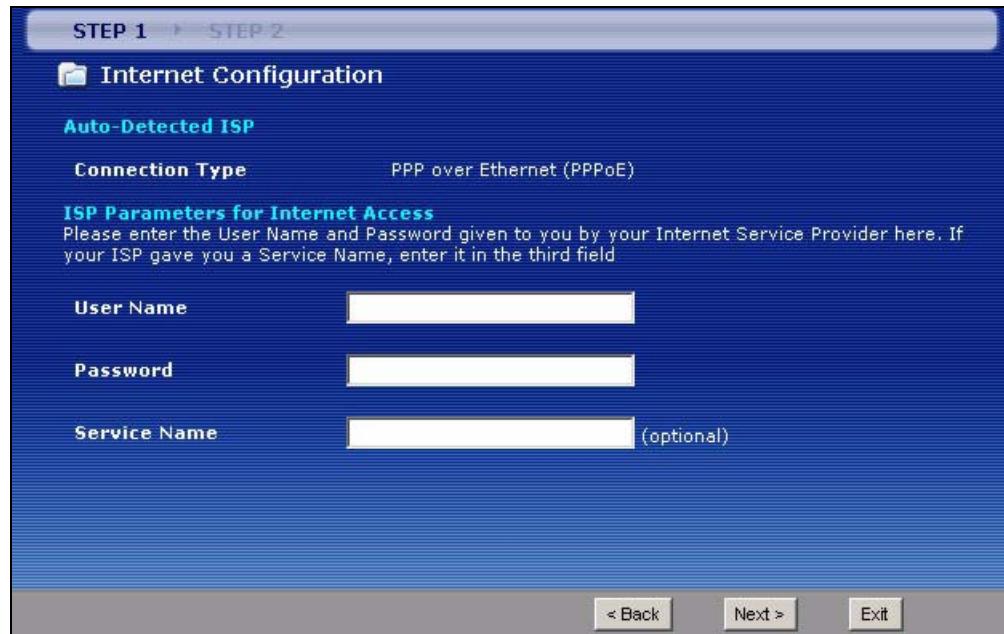
Figure 14 Wizard Welcome

3 Your ZyXEL device attempts to detect your DSL connection and your connection type.

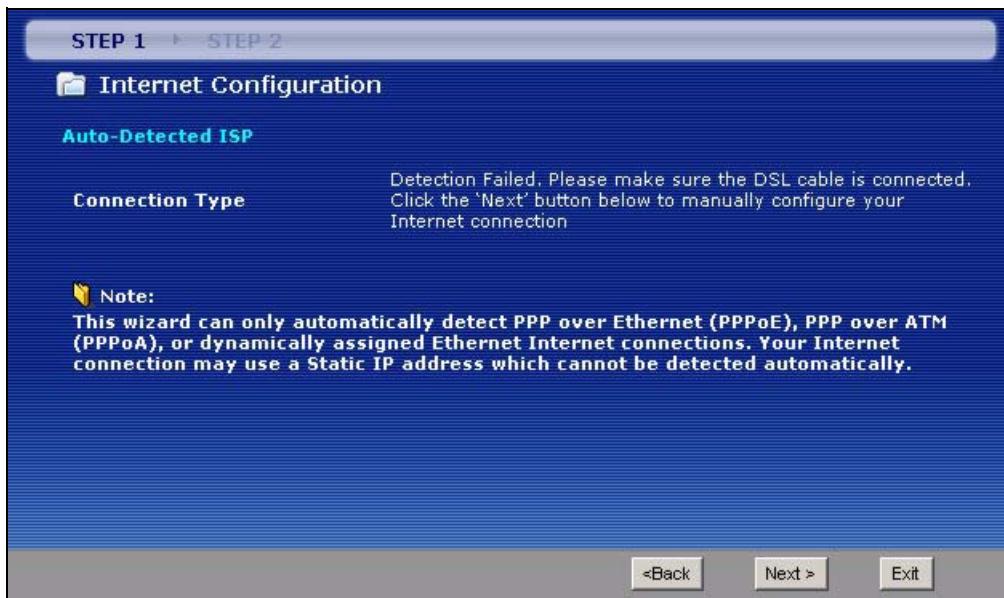
- a** The following screen appears if a connection is not detected. Check your hardware connections and click **Restart the Internet/Wireless Setup Wizard** to return to the wizard welcome screen.
If you would like to skip your Internet setup and configure the wireless LAN settings, leave **Yes** selected and click **Next**.
If you would like to select your Internet settings yourself, click **Manually Configure your Internet connection**. Refer to [Section 3.2.1 on page 63](#) for more information.

Figure 15 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. Then click **Next** and see [Section 3.3 on page 69](#) for wireless connection wizard setup.

Figure 16 Auto-Detection: PPPoE

- 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 63](#) on how to manually configure the ZyXEL Device for Internet access.

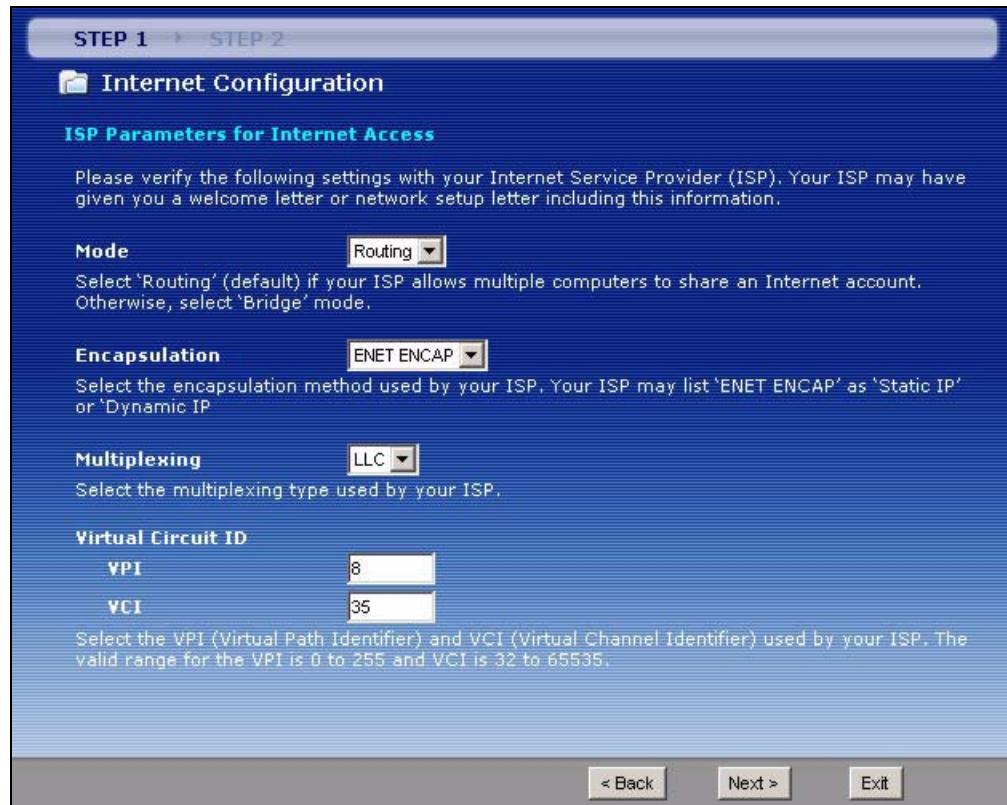
Figure 17 Auto Detection: Failed

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

ISP gave it to you. Leave the defaults in any fields for which you were not given information.

Figure 18 Internet Access Wizard Setup: ISP Parameters



The following table describes the fields in this screen.

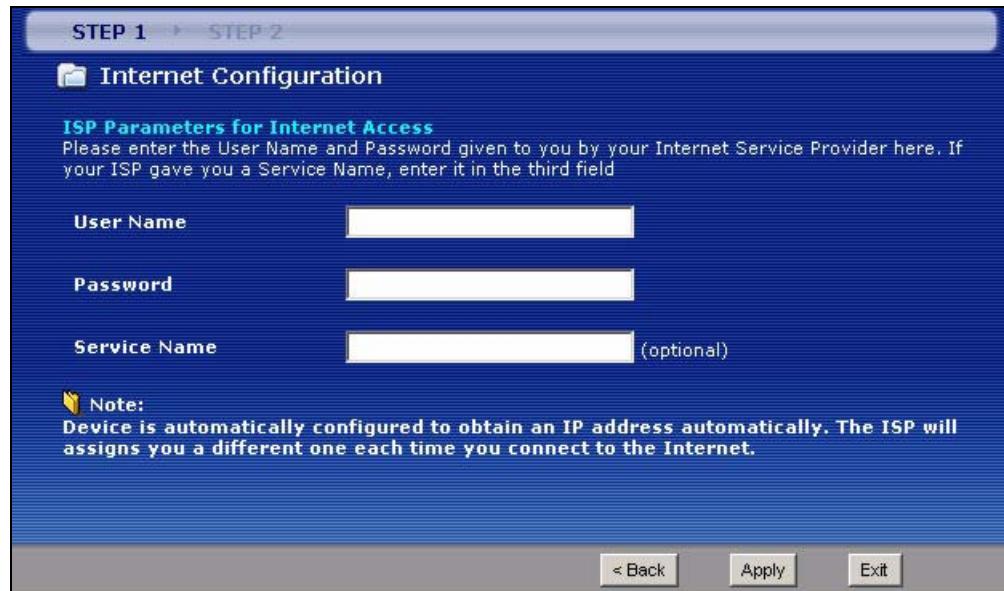
Table 7 Internet Access Wizard Setup: ISP Parameters

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 Multiplexing 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 Appendix E on page 391 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.

Table 7 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Next	Click Next to continue to the next wizard screen. The next wizard screen you see depends on what encapsulation you chose above.
Exit	Click Exit to close the wizard screen without saving your changes.

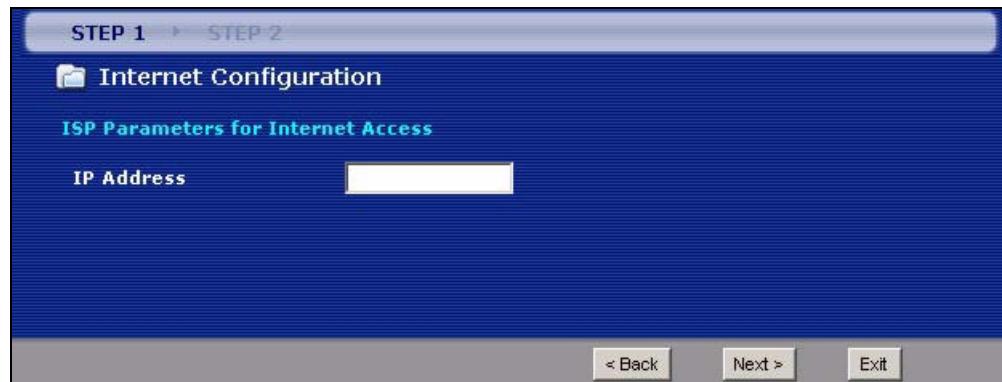
- 2** The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue. See [Section 3.3 on page 69](#) for wireless connection wizard setup

Figure 19 Internet Connection with PPPoE

The following table describes the fields in this screen.

Table 8 Internet Connection with PPPoE

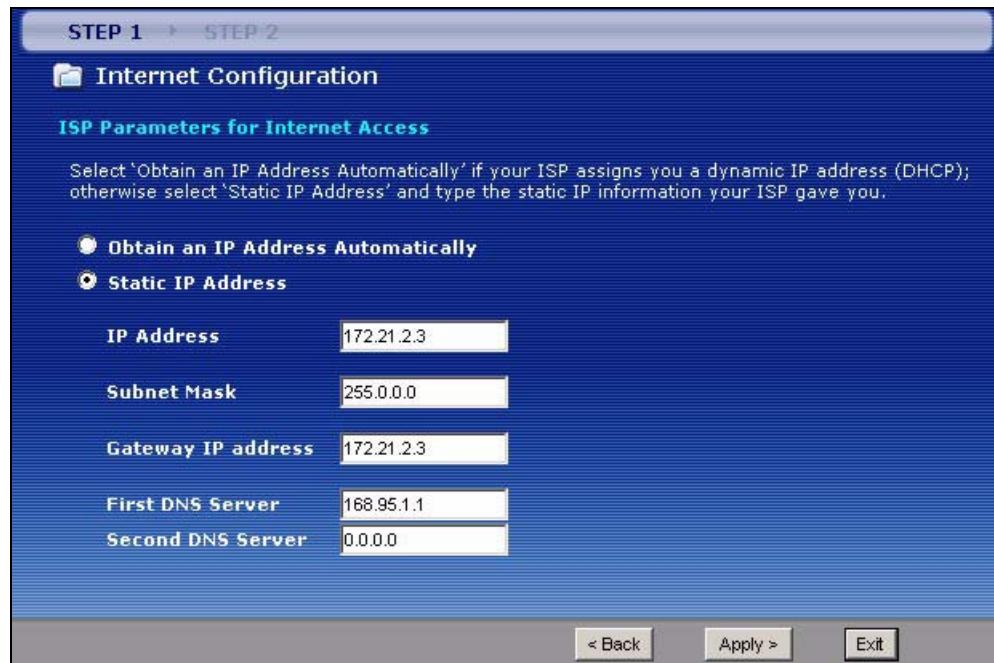
LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Service Name	Type the name of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

Figure 20 Internet Connection with RFC 1483

The following table describes the fields in this screen.

Table 9 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 21 Internet Connection with ENET ENCAP

The following table describes the fields in this screen.

Table 10 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 appendices 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 to the ZyXEL Device.
Exit	Click Exit to close the wizard screen without saving your changes.

Figure 22 Internet Connection with PPPoA

The following table describes the fields in this screen.

Table 11 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.
Back	Click Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes 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.

Figure 23 Connection Test Failed-1

- 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. Click **Manually configure your Internet connection** to return to the manual configuration screen.

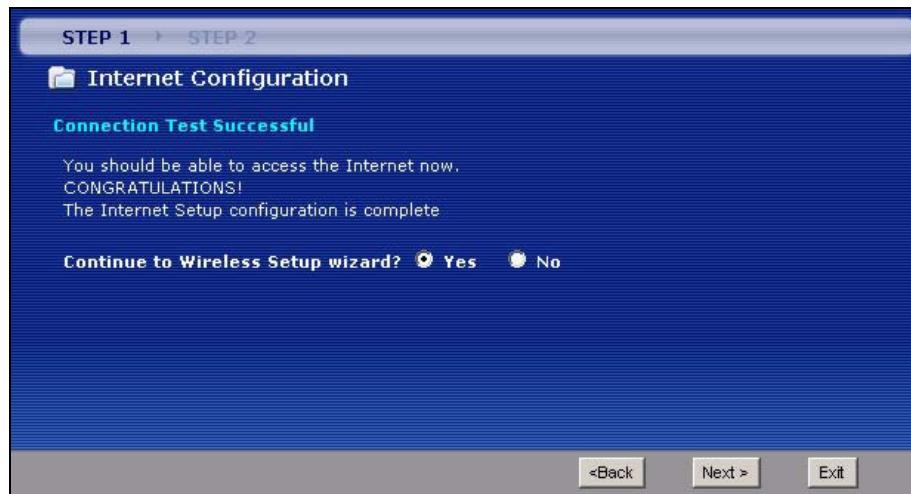
Figure 24 Connection Test Failed-2.

3.3 Wireless Connection Wizard Setup

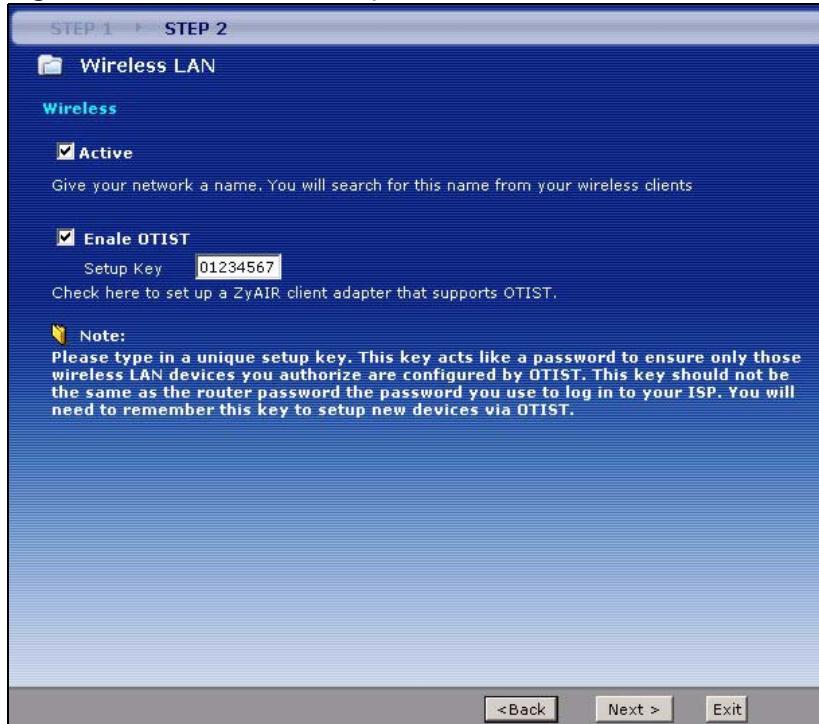
After you configure the Internet access information, use the following screens to set up your wireless LAN.

- 1 Select **Yes** and click **Next** to configure wireless settings. Otherwise, select **No** and skip to Step 6.

Figure 25 Connection Test Successful



2 Use this screen to activate the wireless LAN and OTIST. Click **Next** to continue.

Figure 26 Wireless LAN Setup Wizard 1

The following table describes the labels in this screen.

Table 12 Wireless LAN Setup Wizard 1

LABEL	DESCRIPTION
Active	Select the check box to turn on the wireless LAN.
Enable OTIST	Select the check box to enable OTIST if you want to transfer your ZyXEL Device's SSID and WEP or WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You must also activate and start OTIST on the wireless client at the same time. The process takes three minutes to complete.
Setup Key	Type an OTIST Setup Key of up to eight ASCII characters in length. Be sure to use the same OTIST Setup Key on the ZyXEL Device and wireless clients.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

3 Configure your wireless settings in this screen. Click **Next**.

Figure 27 Wireless LAN

The following table describes the labels in this screen.

Table 13 Wireless LAN Setup Wizard 2

LABEL	DESCRIPTION
Network Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyXEL Device, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device.
Security	Select Manually assign a WPA-PSK key to configure a Pre-Shared Key (WPA-PSK). Choose this option only if your wireless clients support WPA. See Section 3.3.1 on page 73 for more information. Select Manually assign a WEP key to configure a WEP Key. See Section 3.3.2 on page 73 for more information. Select Disable wireless security to have no wireless LAN security configured and your network is accessible to any wireless networking device that is within range. Select Static WEP (User configured) if you have configured the WEP key before.
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.

Note: The wireless stations and ZyXEL Device must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) for wireless communication.

- 4 This screen varies depending on the security mode you selected in the previous screen.
Fill in the field (if available) and click **Next**.

3.3.1 Manually Assign a WPA key

Choose **Manually assign a WPA key** in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 28 Manually Assign a WPA key



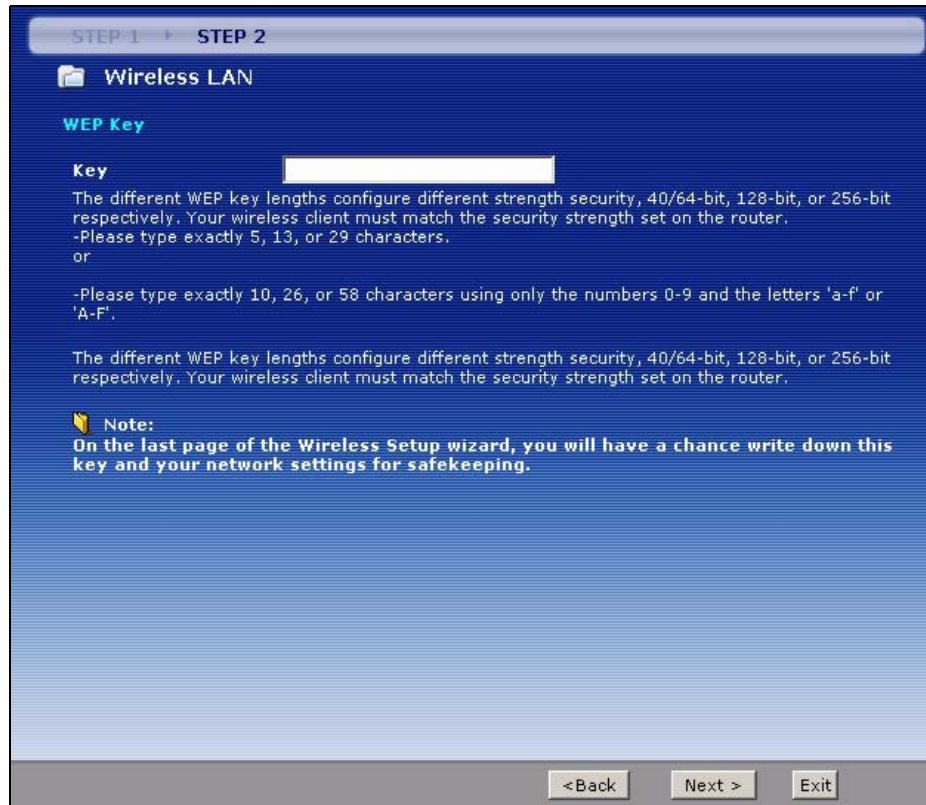
The following table describes the labels in this screen.

Table 14 Manually Assign a WPA key

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

3.3.2 Manually Assign a WEP key

Choose **Manually assign a WEP key** to setup WEP encryption parameters.

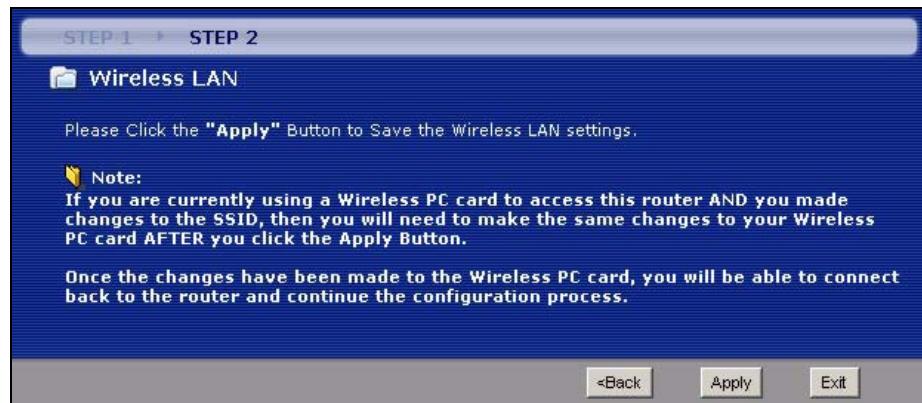
Figure 29 Manually Assign a WEP key

The following table describes the labels in this screen.

Table 15 Manually Assign a WEP key

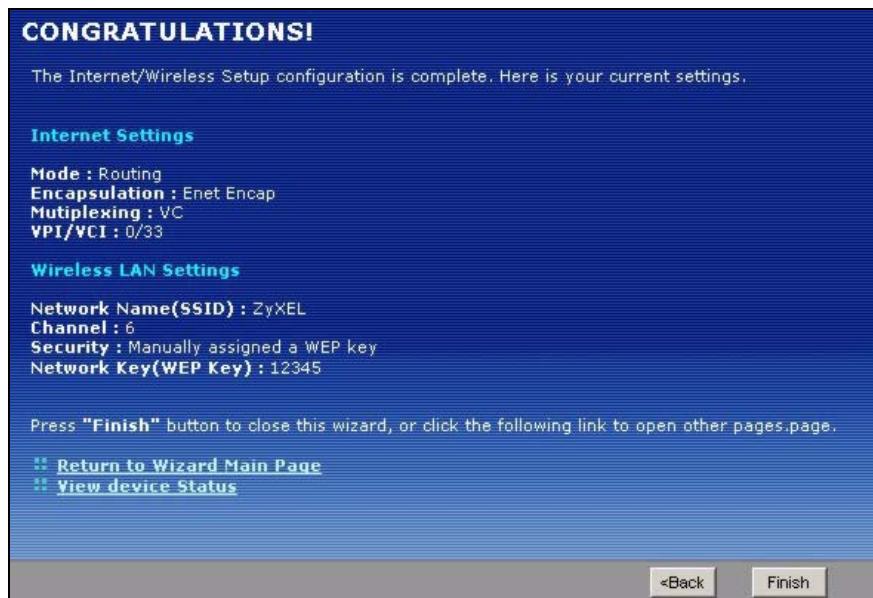
LABEL	DESCRIPTION
Key	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. Enter any 5, 13 or 29 ASCII characters or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively.
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.

5 Click **Apply** to save your wireless LAN settings.

Figure 30 Wireless LAN Setup 3

- 6** Use the read-only summary table to check whether what you have configured is correct.
Click **Finish** to complete and save the wizard setup.

Note: No wireless LAN settings display if you chose not to configure wireless LAN settings.

Figure 31 Internet Access and WLAN Wizard Setup Complete

- 7** Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

CHAPTER 4

VoIP Wizard

This chapter shows you how to configure your device to use the wizard to configure your device to use your SIP account(s).

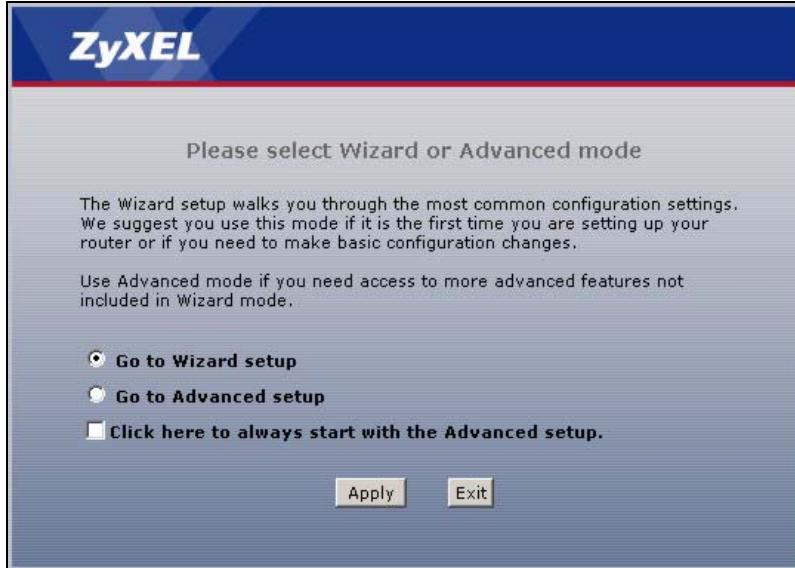
4.1 Introduction

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

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 (wizard icon) in the top right corner of the web configurator to display the wizard main screen.

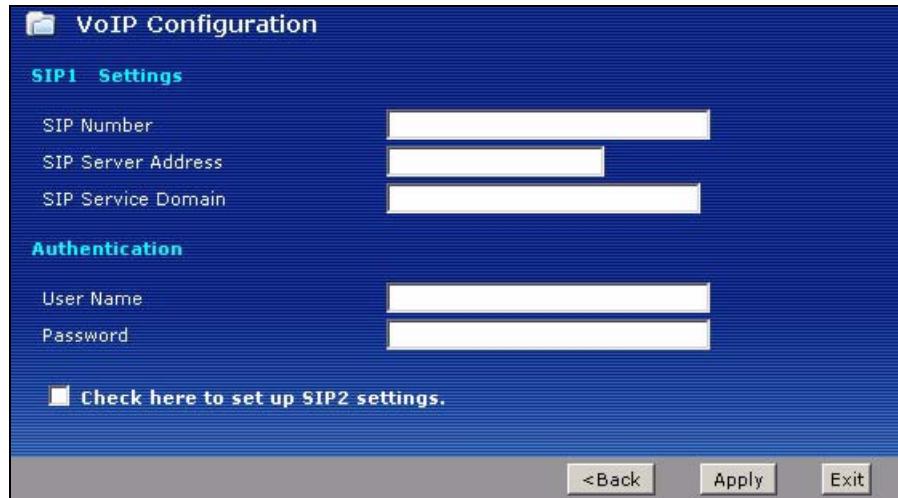
Figure 32 Select a Mode



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

Figure 33 Wizard: Welcome

- 3 This wizard screen allows you to configure your voice settings for SIP account 1. Fill in the fields with information from your VoIP service provider. Leave the default settings in fields for which no information was provided (except if otherwise specified). See [Chapter 11 on page 165](#) for background information on these fields.

Figure 34 VOIP Wizard Configuration

The following table describes the labels in this screen

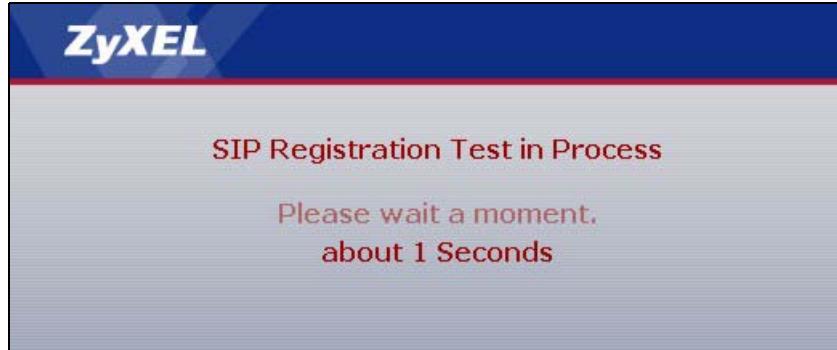
Table 16 VOIP Wizard Configuration

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 like 1234@VoIP-provider.com). 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.
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 1234@VoIP-provider.com). You can use up to 127 ASCII Extended set characters.
User Name	This is the user name for registering 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.

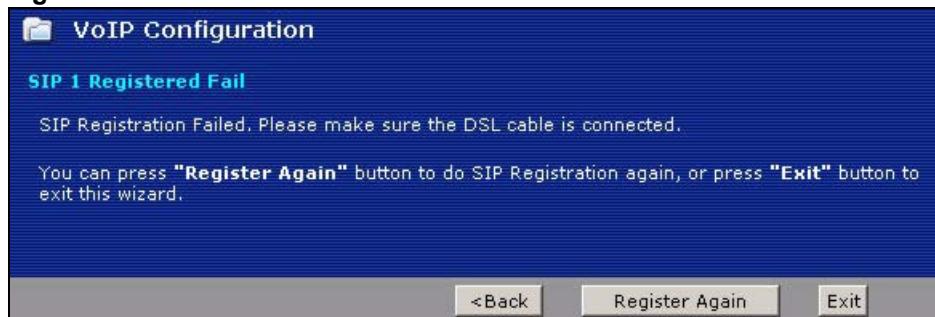
Table 16 VOIP Wizard Configuration

LABEL	DESCRIPTION
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.
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 The ZyXEL Device attempts to register your SIP account with the SIP server.

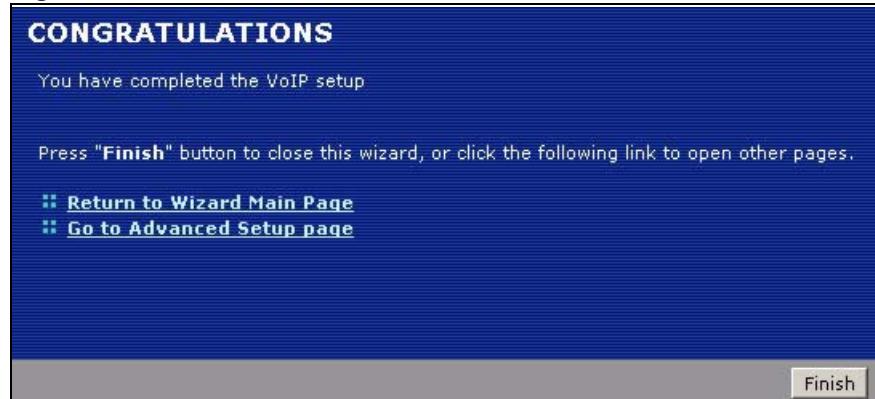
Figure 35 SIP Registration Test

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 36 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 37 VOIP Wizard Finish



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 interfaces 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 17 Media Bandwidth Management Setup: Services

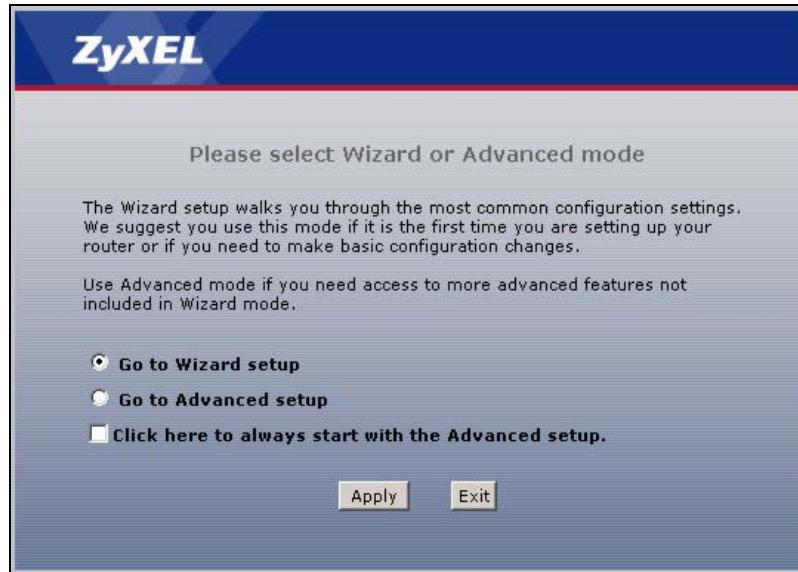
SERVICE	DESCRIPTION
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the 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 17 Media Bandwidth Management Setup: Services (continued)

SERVICE	DESCRIPTION
NetMeeting (H.323)	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. 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. H.323 is transported primarily over TCP, using the default port number 1720.
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.
VoIP (H.323)	Sending voice signals over the Internet is called Voice over IP or VoIP. 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. H.323 is transported primarily over TCP, using the default port number 1720.
TFTP	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).

5.3 Bandwidth Management Wizard Setup

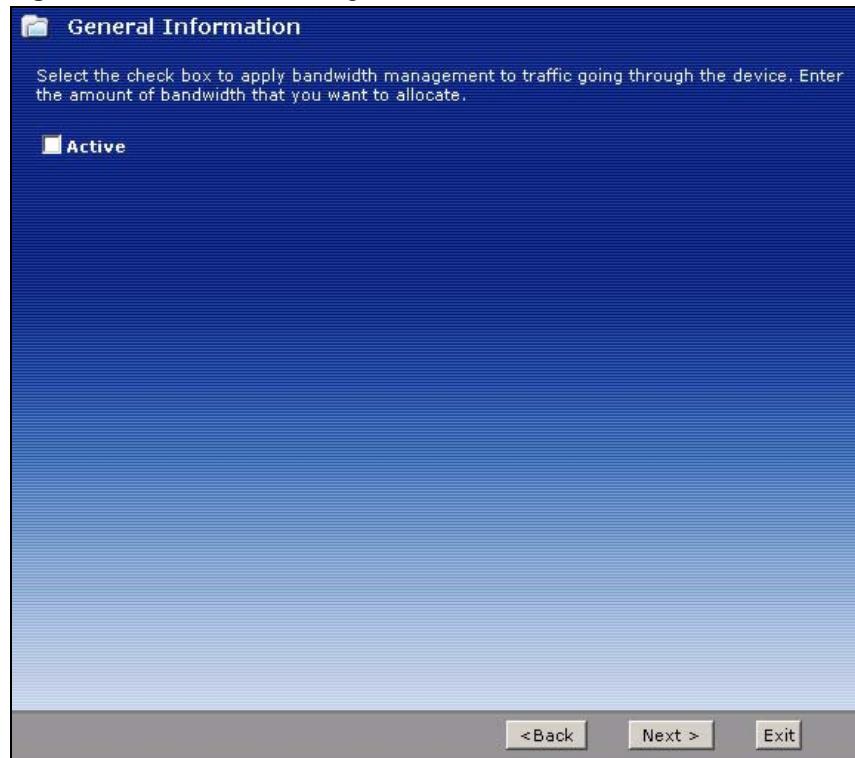
- 1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon () in the top right corner of the web configurator to display the wizard main screen.

Figure 38 Select a Mode

2 Click BANDWIDTH MANAGEMENT SETUP.

Figure 39 Wizard: Welcome

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

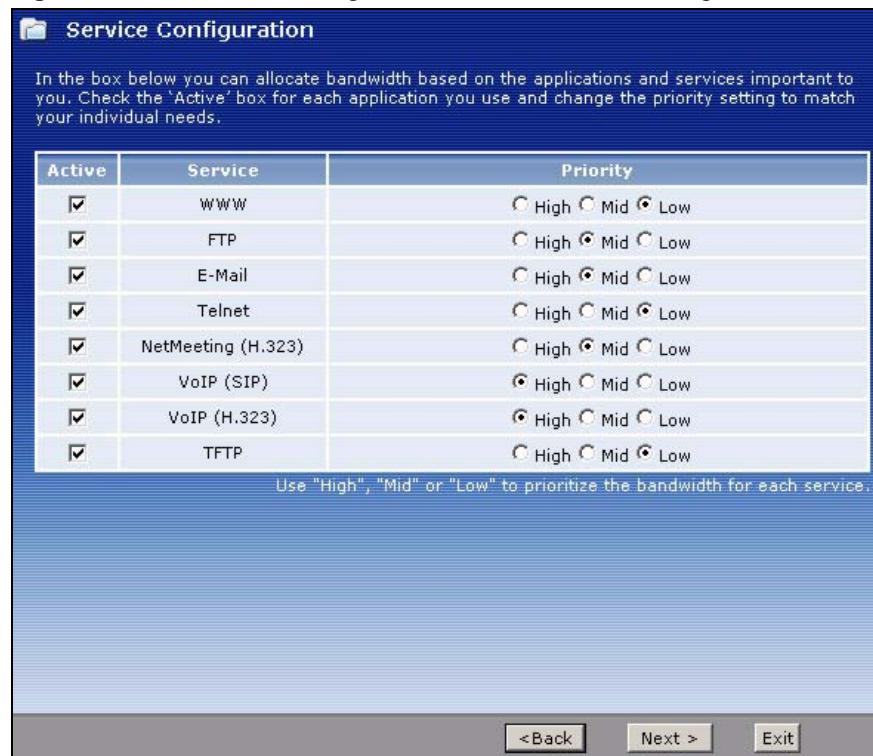
Figure 40 Bandwidth Management Wizard: General Information

The following fields describe the label in this screen.

Table 18 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, LAN or WLAN port.
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.

- 4 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 41 Bandwidth Management Wizard: Service Configuration

The following table describes the labels in this screen.

Table 19 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.
Priority	Select High , Mid or Low priority for each service to have your ZyXEL Device use a priority for traffic that matches that service. A service with High priority is given as much bandwidth as it needs. If you select services as having the same priority, then bandwidth is divided equally amongst those services. Services not specified in bandwidth management are allocated bandwidth after all specified services receive their bandwidth requirements. 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 . The Advanced , Bandwidth MGMT , Rule Setup screen allows you to edit these rule configurations.
Back	Click Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes 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 42 Bandwidth Management Wizard: Complete



CHAPTER 6

WAN Setup

This chapter describes how to configure WAN settings.

6.1 WAN Overview

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

6.1.1 Encapsulation

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

6.1.1.1 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. You can get this information from your ISP.

6.1.1.2 PPP over Ethernet

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

6.1.1.3 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.

6.1.1.4 RFC 1483

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

6.1.2 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.

6.1.2.1 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.

6.1.2.2 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.

6.1.3 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.

6.1.4 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. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

6.1.4.1 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.

6.1.4.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP address assignment *must* be static.

6.1.4.3 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.

6.1.5 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

6.2 PPPoE Encapsulation

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.

6.3 Metric

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

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

- Normal route: designated by the ISP (see [Section 6.6 on page 92](#))
- Traffic-redirect route (see [Section 6.10 on page 100](#))
- WAN-backup route, also called dial-backup (see [Section 6.10 on page 100](#))

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.

6.4 Traffic Shaping

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

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

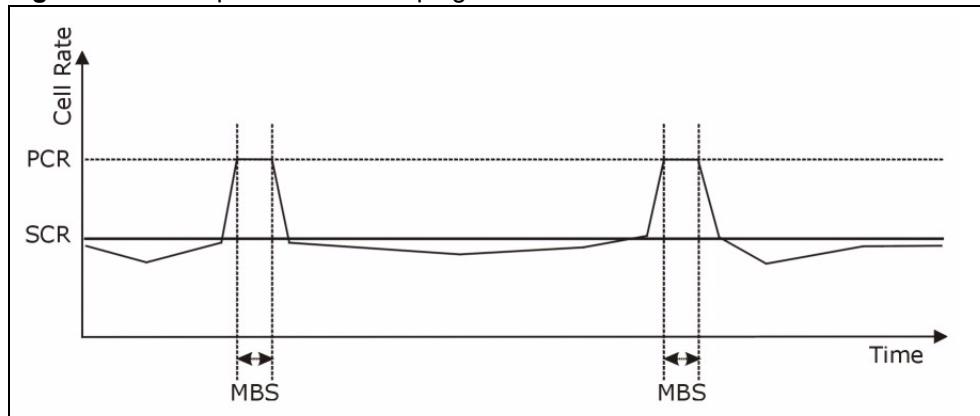
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

Figure 43 Example of Traffic Shaping



6.4.1 ATM Traffic Classes

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

6.4.1.1 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.

6.4.1.2 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.

6.4.1.3 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.

6.5 Zero Configuration Internet Access

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

Zero configuration for Internet access is disabled when

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

6.6 Internet Access Setup

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

See [Section 6.1 on page 87](#) for more information.

Figure 44 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.

Table 20 Internet Access Setup (continued)

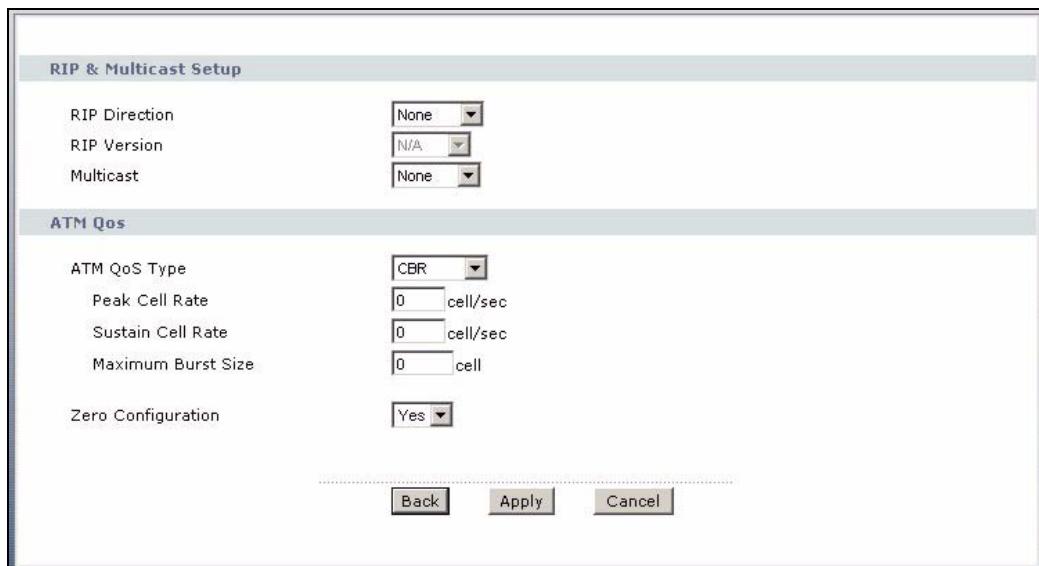
LABEL	DESCRIPTION
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC .
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	This option is available if you select Routing in the Mode field.
Obtain an IP Address Automatically	Select Obtain an IP Address Automatically if you have a dynamic IP address. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Static IP Address	A static IP address is a fixed IP that your ISP gives you. Type your ISP assigned IP address in the IP Address field below.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
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	
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.
First DNS Server Second DNS Server Third DNS Server	Select Obtained from ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right. Select UserDefined 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 UserDefined , but leave the IP address set to 0.0.0.0, UserDefined changes to None after you click Apply . If you set a second choice to UserDefined , and enter the same IP address, the second UserDefined changes to None after you click Apply . 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.
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.
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.

Table 20 Internet Access Setup (continued)

LABEL	DESCRIPTION
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.

6.6.1 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 45 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 bursty connections that require closely controlled delay and delay variation. Select VBR-nRT (non real-time Variable Bit Rate) for bursty 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.

6.7 Configuring More Connections

This section describes the protocol-independent parameters for a remote network. They are required for placing calls to a remote gateway and the network behind it across a WAN connection. When you use the **WAN > Internet Connection** screen to set up Internet access, you are configuring the first WAN connection.

Click **Network > WAN > More Connections** to display the screen as shown next.

Figure 46 More Connections

More Connections					
#	Active	Name	VPI/VCI	Encapsulation	Modify
1	-	Internet Connection	1/32	PPPoA	
2	-	--	--	--	
3	-	--	--	--	
4	-	--	--	--	
5	-	--	--	--	
6	-	--	--	--	
7	-	--	--	--	
8	-	--	--	--	

Apply **Cancel**

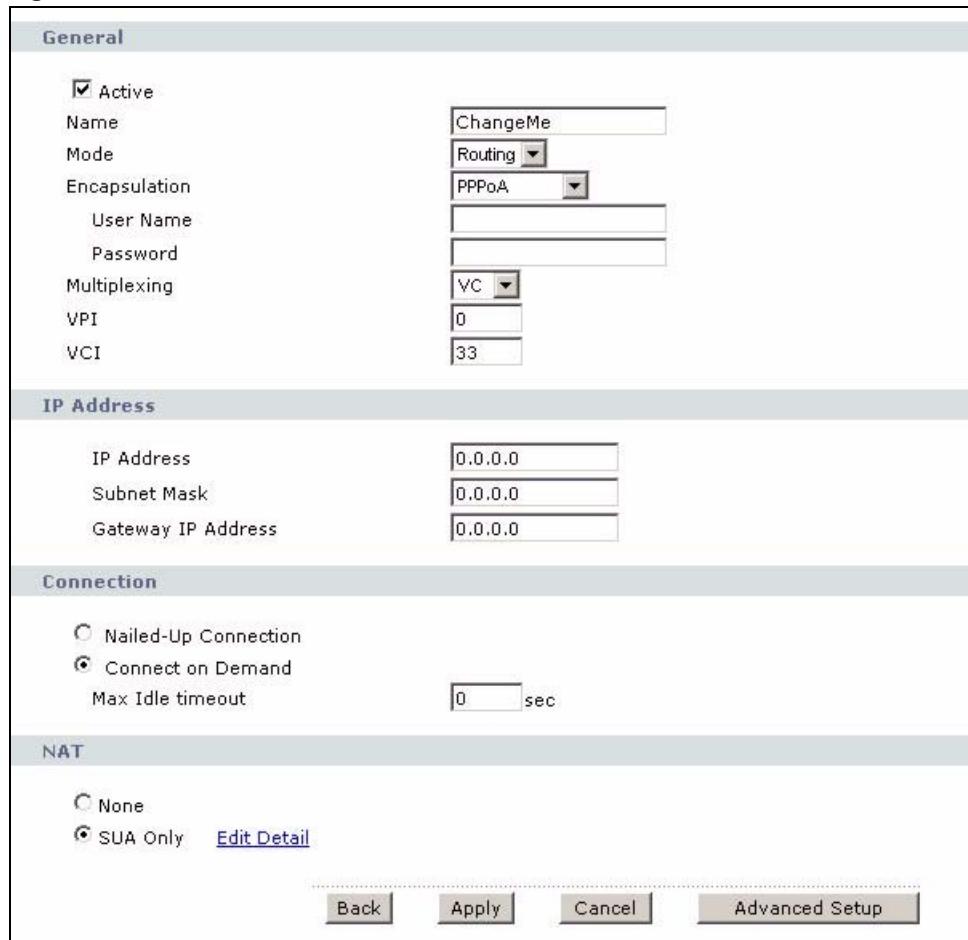
The following table describes the labels in this screen.

Table 22 More Connections

LABEL	DESCRIPTION
#	This is the index number of a connection.
Active	This displays whether this connection is activated. Clear the check box to disable the connection. Select the check box to enable it.
Name	This is the descriptive name for this connection.
VPI/VCI	This is the VPI and VCI values used for this connection.
Encapsulation	This is the method of encapsulation used for this connection.
Modify	The first (ISP) connection is read-only in this screen. Use the WAN > Internet Connection screen to edit it. Click the edit icon to go to the screen where you can edit the connection. Click the delete icon to remove an existing connection. You cannot remove the first connection.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.8 More Connections Edit

Click the edit icon in the **More Connections** screen to configure a node.

Figure 47 More Connections Edit

The following table describes the labels in this screen.

Table 23 More Connections Edit

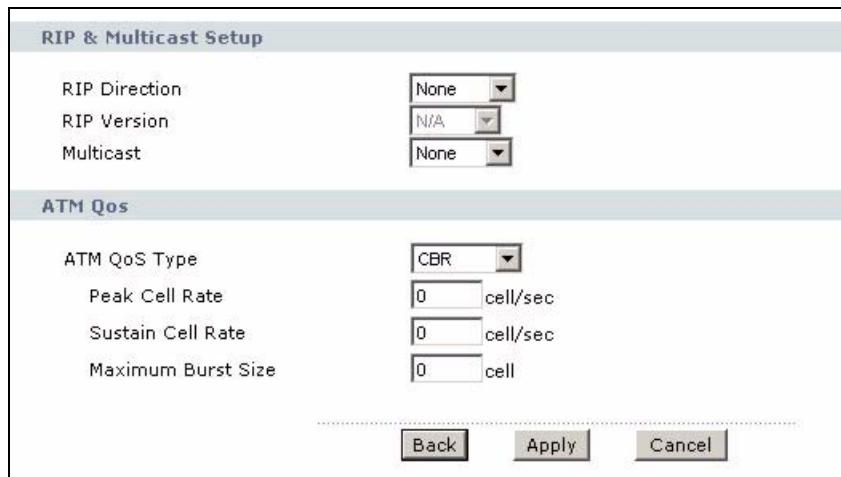
LABEL	DESCRIPTION
Active	Select the check box to activate or clear the check box to deactivate this node.
Name	Enter a unique, descriptive name of up to 20 characters for this node. You can use alphanumeric characters and the hyphen “-”, underscore “_” and @.
General	
Mode	Select Routing from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select Bridge , the ZyXEL Device will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices are 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 23 More Connections Edit (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 . By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol. For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.
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	This option is available if you select Routing in the Mode field. Type your (static) ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask if you are implementing subnetting.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
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.
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.
NAT	SUA only and Full Feature are available only when you select Routing in the Mode field. Select SUA Only if you have one public IP address, Full Feature if you have multiple public IP addresses (for address translation) or None to disable NAT. When selecting Full Feature , configure address mapping sets in the Address Mapping screen. Select one of the NAT server sets (2-10) in the Port Forwarding screen (see Chapter 10 on page 153 for details) and type that number here.
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.
Advanced Setup	Click this button to edit RIP, multicast and ATM QoS settings.

6.9 More Connections Edit Advanced

Click the **Advanced** button in the **More Connections Edit** screen to display the following screen.

Figure 48 More Connections Edit Advanced

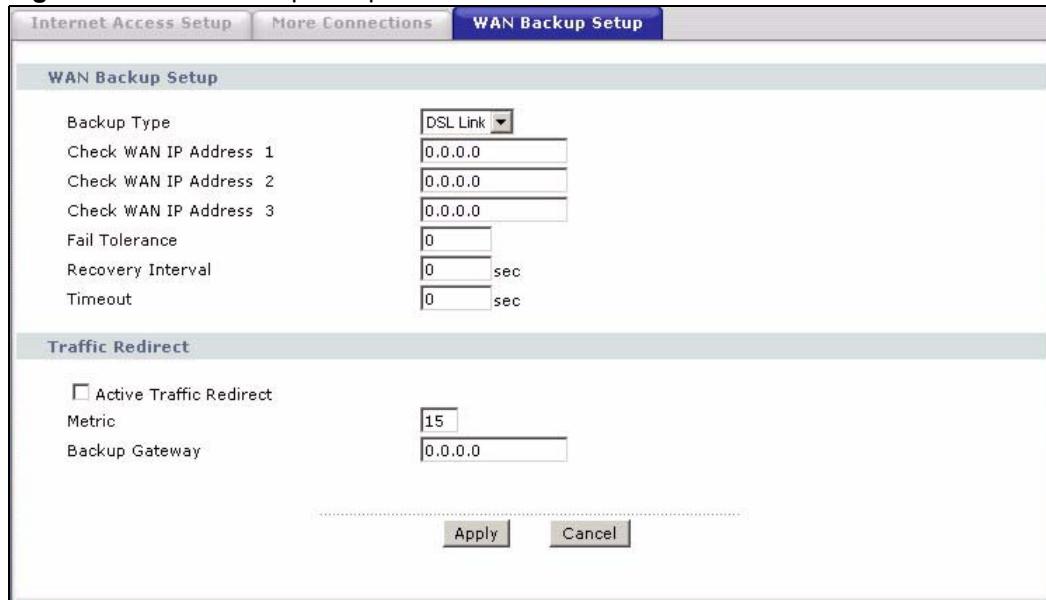
The following table describes the labels in this screen.

Table 24 More Connections Edit Advanced

LABEL	DESCRIPTION
RIP Direction	Select the RIP direction from None , Both , In Only and Out Only .
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 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 (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
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.
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.

6.10 Configuring WAN Backup

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

Figure 49 WAN Backup Setup

The following table describes the labels in this screen.

Table 25 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.

Table 25 WAN Backup Setup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the 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.

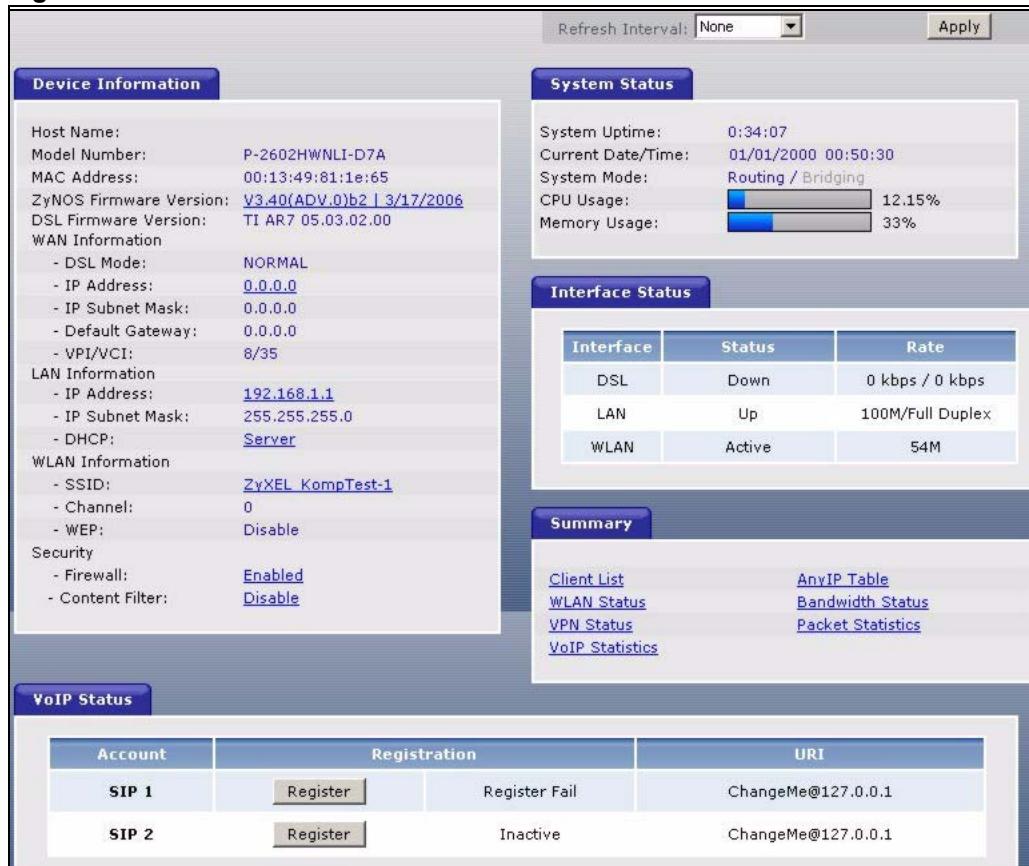
CHAPTER 7

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.

7.1 Status Screen

Click **Status** to open this screen.

Figure 50 Status Screen

Each field is described in the following table.

Table 26 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Refresh Now	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. You can change the firmware version by uploading new firmware in Maintenance > Tools > Firmware .
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.

Table 26 Status Screen

LABEL	DESCRIPTION
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.
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 is routing DHCP requests to one or more DHCP servers. The DHCP server(s) may be on another network. None - The ZyXEL Device is not providing any DHCP services to the LAN. You can change this in Network > LAN > DHCP Setup .
WLAN Information	
SSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN.
Channel	This is the channel number used by the ZyXEL Device now.
WEP	This displays the status of WEP data encryption.
Security	
Firewall	This displays whether or not the ZyXEL Device's firewall is activated.
Content Filter	This displays whether or not the ZyXEL Device's content filtering is activated.
System Status	
System Up Time	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 55).
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. The higher the CPU usage, the more likely the ZyXEL Device slows down. You can reduce this by disabling some services, such as DHCP, NAT, or content filtering.
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. The higher the memory usage, the more likely the ZyXEL Device slows down. Some memory is required just to start the ZyXEL Device and to run the web configurator. You can reduce the memory usage by disabling some services (see CPU Usage); by reducing the amount of memory allocated to NAT and firewall rules (you may have to reduce the number of NAT rules or firewall rules to do so); or by deleting rules in functions such as incoming call policies, speed dial entries, and static routes.
Interface Status	

Table 26 Status Screen

LABEL	DESCRIPTION
Interface	This column displays each interface the ZyXEL Device has.
Status	For the DSL interface, this field displays Down (line is down), Detect Signal (checking DSL connection), or Up (line is up or connected) if you're using Ethernet encapsulation and Down (line is down), Detect Signal (checking DSL connection), 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. For the WLAN port, it displays Active when WLAN is enabled or Inactive when WLAN is disabled.
Rate	For the LAN ports this displays the port speed and duplex setting. For the DSL port, it displays the downstream and upstream transmission rate. For the WLAN port, it displays the transmission rate when WLAN is enabled or N/A when WLAN is disabled.
Summary	
Client List	Click this link to view current DHCP client information.
Any IP 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.
WLAN Status	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device.
VPN Status	Use this screen to view the status of any VPN tunnels the ZyXEL Device has negotiated.
Bandwidth Status	Click this link to view the ZyXEL Device's bandwidth usage and allotments.
Packet Statistics	Click this link to view port status and packet specific statistics.
VoIP Statistics	Click this link to view statistics about your VoIP usage.
VoIP Status	
Account	This column displays each SIP account in the ZyXEL Device.

Table 26 Status Screen

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. If the SIP account is already registered with the SIP server, 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 . If the SIP account is not registered with the SIP server, 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. Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Settings . 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.
URI	This field displays the account number and service domain of the SIP account. You can change these in VoIP > SIP > SIP Settings .

7.2 Client List

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

Click **Status > Client List** to access this screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyXEL Device's DHCP server.

Figure 51 Client List

The following table describes the labels in this screen.

Table 27 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 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 host computer.
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 an entry to have the ZyXEL Device always assign the selected entry's IP address to the corresponding MAC address (and host name). After you click Apply , the MAC address and IP address also display in the LAN Static DHCP screen (where you can edit them).
Modify	The edit icon is available only when you select the Reserve check box. Click the edit icon to make the IP address field editable and change it.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.
Refresh	Click Refresh to reload the DHCP table.

7.3 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 52 Any IP Table

Any IP TABLE		
#	IP Address	MAC Address
.....		
		Refresh

Each field is described in the following table.

Table 28 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.
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.

7.4 WLAN Status

Click **Status > WLAN Status** to access this screen. Use this screen to view the wireless stations that are currently associated to the ZyXEL Device.

Figure 53 WLAN Status

Wireless LAN- Association List		
#	MAC Address	Association Time
1	00:ac:c5:01:23:45	1
Refresh		

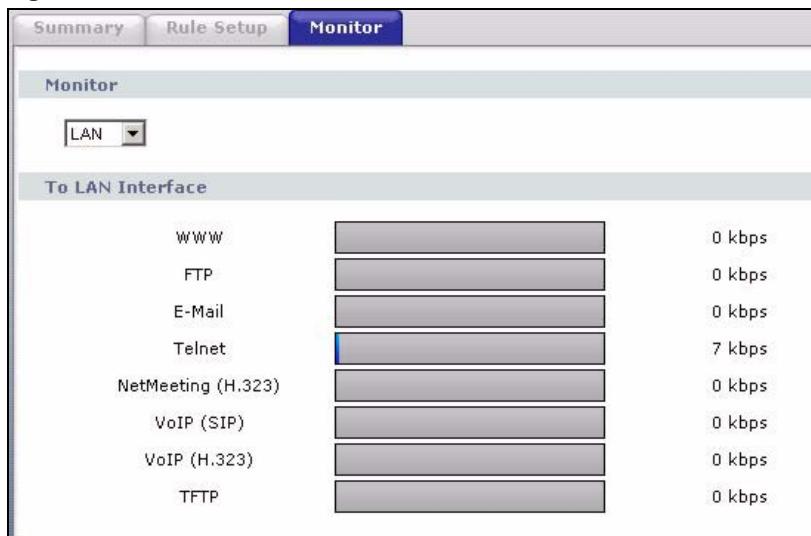
The following table describes the labels in this screen.

Table 29 WLAN Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
Refresh	Click Refresh to reload this screen.

7.4.1 Bandwidth Status

Click **Status > Bandwidth Status** to access this screen. Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth rules. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 54 Bandwidth Status

7.4.2 VPN Status

Click **Status > VPN Status** to access this screen. The **VPN Status** screen shows the current status of any VPN tunnels the ZyXEL Device has negotiated.

Figure 55 Status: VPN Status

The screenshot shows a software interface titled "Status: VPN Status". At the top, there are three tabs: "Setup", "Monitor" (which is selected and highlighted in blue), and "VPN Global Setting". Below the tabs is a table with 20 rows, each representing a security association (SA). The columns are labeled "No.", "Name", "Encapsulation", and "IP Sec Algorithm". All entries in the table are currently empty or show a dash (-) in every field. At the bottom of the screen are two buttons: "Disconnect" and "Refresh".

No.	Name	Encapsulation	IP Sec Algorithm
1	-	-	-
2	-	-	-
3	-	-	-
4	-	-	-
5	-	-	-
6	-	-	-
7	-	-	-
8	-	-	-
9	-	-	-
10	-	-	-
11	-	-	-
12	-	-	-
13	-	-	-
14	-	-	-
15	-	-	-
16	-	-	-
17	-	-	-
18	-	-	-
19	-	-	-
20	-	-	-

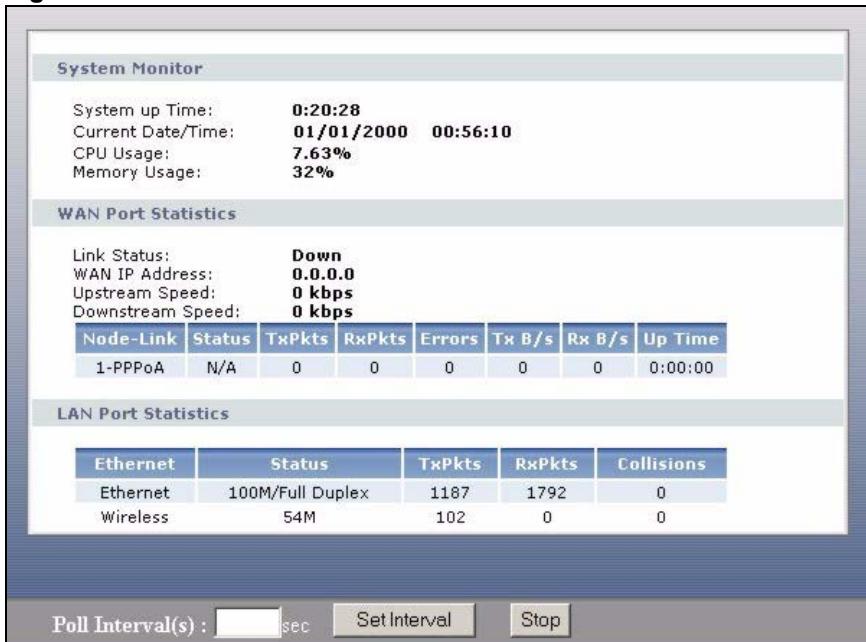
The following table describes the labels in this screen.

Table 30 Status: VPN Status

LABEL	DESCRIPTION
No	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays Tunnel or Transport mode.
IPSec Algorithm	This field displays the security protocol, encryption algorithm, and authentication algorithm used in each SA.
Disconnect	Select one of the security associations, and then click Disconnect to stop that security association.
Refresh	Click Refresh to display the current active VPN connection(s).

7.5 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 56 Packet Statistics

The following table describes the fields in this screen.

Table 31 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.
LAN or WAN Port Statistics	This is the WAN or LAN port.
Link Status	This is the status of your WAN link.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Ethernet	This field displays the type of port.
Status	This field displays Down (line is down), Detect Signal (checking DSL connection) or Up (line is up or connected) if you're using Ethernet encapsulation and Down (line is down), Detect Signal (checking DSL connection), Up (line is up or connected), Idle (line (ppp) idle), Dial (starting to trigger a call) or Drop (dropping a call) if you're using PPPoE encapsulation. For the WLAN port, it displays the transmission rate when WLAN is enabled or N/A when WLAN is disabled.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.

Table 31 Packet Statistics (continued)

LABEL	DESCRIPTION
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval field above.
Stop	Click this button to halt the refreshing of the system statistics.

7.6 VoIP Statistics

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

Figure 57 VoIP Statistics

The screenshot shows the VoIP Statistics interface with two main sections: 'SIP Status' and 'Call Statistics'. In the 'SIP Status' section, there are two accounts listed: SIP1 and SIP2, both showing 'Register Fail' status. The 'Call Statistics' section shows two phones: Phone1 and Phone2, both with 'On' status. At the bottom, there is a 'Poll Interval(s)' input field set to 5 seconds, a 'Set Interval' button, and a 'Stop' button.

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

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 32 VoIP Statistics

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.

Table 32 VoIP Statistics

LABEL	DESCRIPTION
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	
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.

Table 32 VoIP Statistics

LABEL	DESCRIPTION
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 8

LAN Setup

This chapter describes how to configure LAN settings.

8.1 LAN Overview

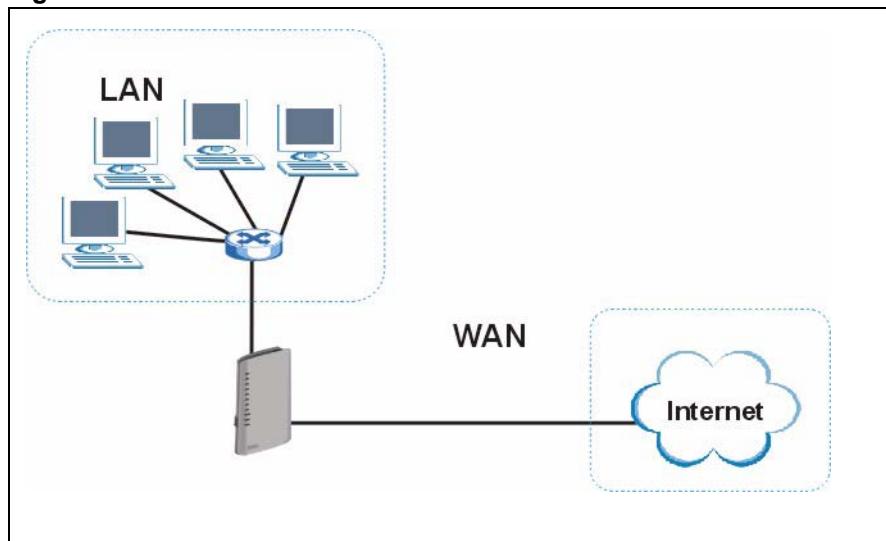
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 8.3 on page 123](#) 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 58 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.

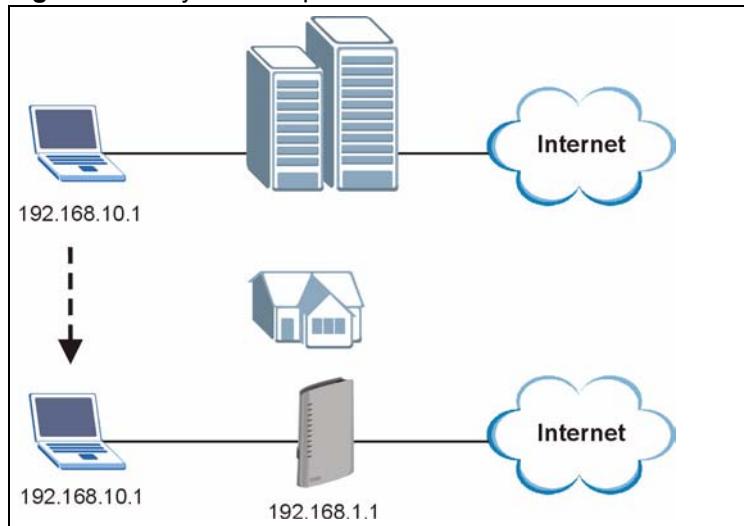
The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on 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 59 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.

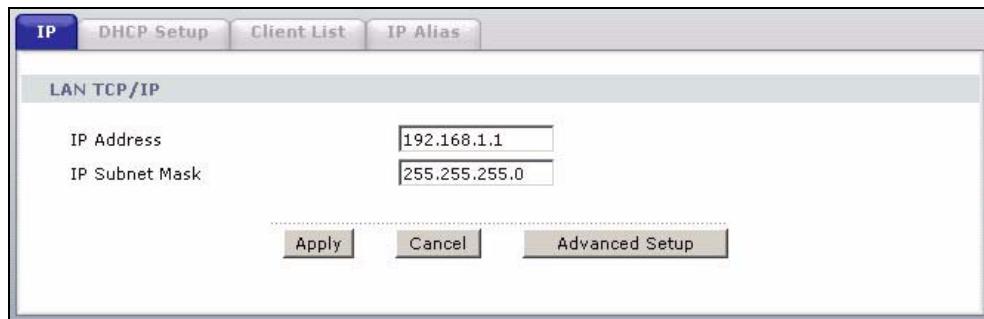
- 1 When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.
- 2 When the computer cannot locate the default gateway, an ARP request is broadcast on the 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 117](#) for background information.

Figure 60 LAN IP



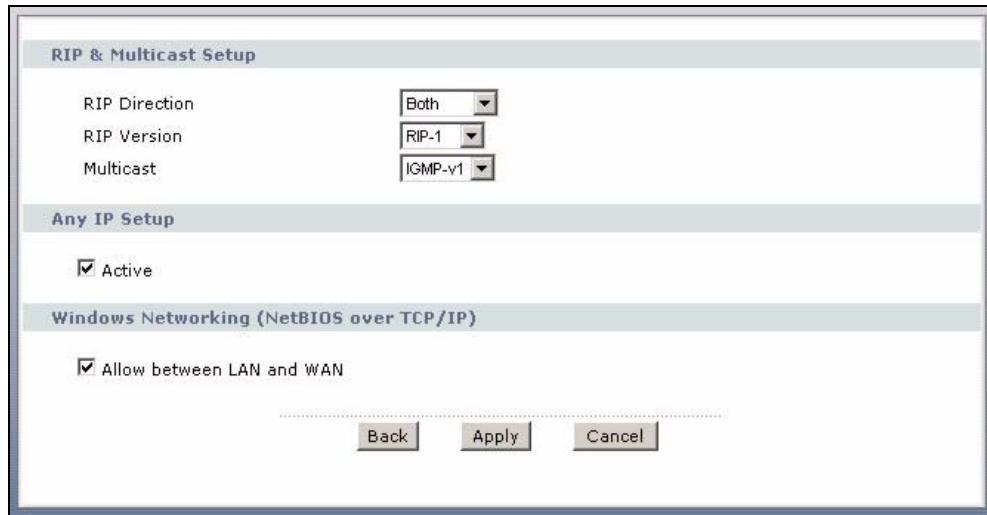
The following table describes the fields in this screen.

Table 33 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 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 61 Advanced LAN Setup

The following table describes the labels in this screen.

Table 34 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 62 DHCP Setup

The screenshot shows the 'DHCP Setup' screen with the following settings:

- DHCP**: Set to **Server**. IP Pool Starting Address is 192.168.1.33. Pool Size is 32. Remote DHCP Server is 0.0.0.0.
- DNS Server**: Three DNS servers are assigned by the DHCP server:
 - First DNS Server: Obtained From ISP (0.0.0.0)
 - Second DNS Server: Obtained From ISP (0.0.0.0)
 - Third DNS Server: Obtained From ISP (0.0.0.0)

Buttons at the bottom: **Apply** and **Cancel**.

The following table describes the labels in this screen.

Table 35 DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	Select what type of DHCP service the ZyXEL Device provides to the network. Choices are: None - the ZyXEL Device does not provide any DHCP services. There is already a DHCP server on the network. Relay - the ZyXEL Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. Server - the ZyXEL Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyXEL Device is the DHCP server for the network.
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.
Remote DHCP Server	Enter the IP address of a DHCP server for the network.
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 35 DHCP Setup

LABEL	DESCRIPTION
First DNS Server	Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right.
Second DNS Server	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 .
Third DNS Server	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 . 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.
Apply	Click Apply to save your changes 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 63 LAN Client List

The screenshot shows a web-based configuration interface for a ZyXEL device. At the top, there are tabs: IP, DHCP Setup, Client List (which is selected and highlighted in blue), and IP Alias. Below the tabs is a header bar with fields for 'IP Address' (192.168.1.66) and 'MAC Address' (AA:BB:CC:EE:EE:EE), and a 'Add' button. The main area is titled 'DHCP Client Table' and contains 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 are three buttons: 'Apply', 'Cancel', and 'Refresh'.

The following table describes the labels in this screen.

Table 36 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	The modify icon is available only when you select the Reserve check box. Click the modify icon to have the IP address field editable and change it.
Apply	Click Apply to save your changes 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

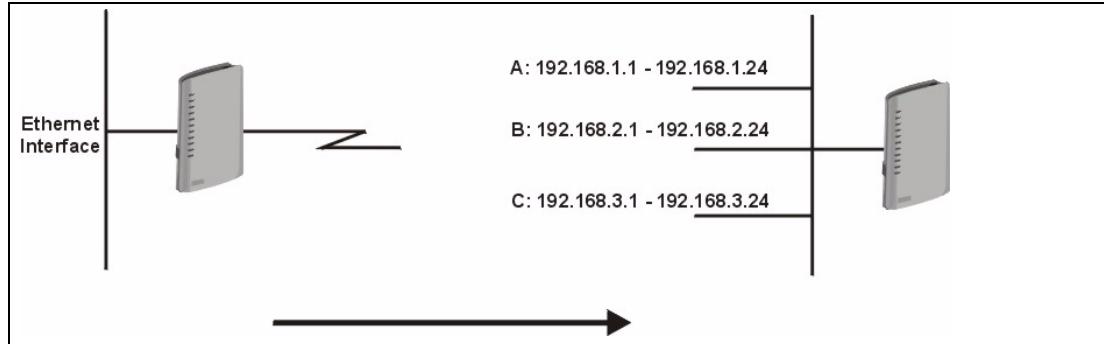
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

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

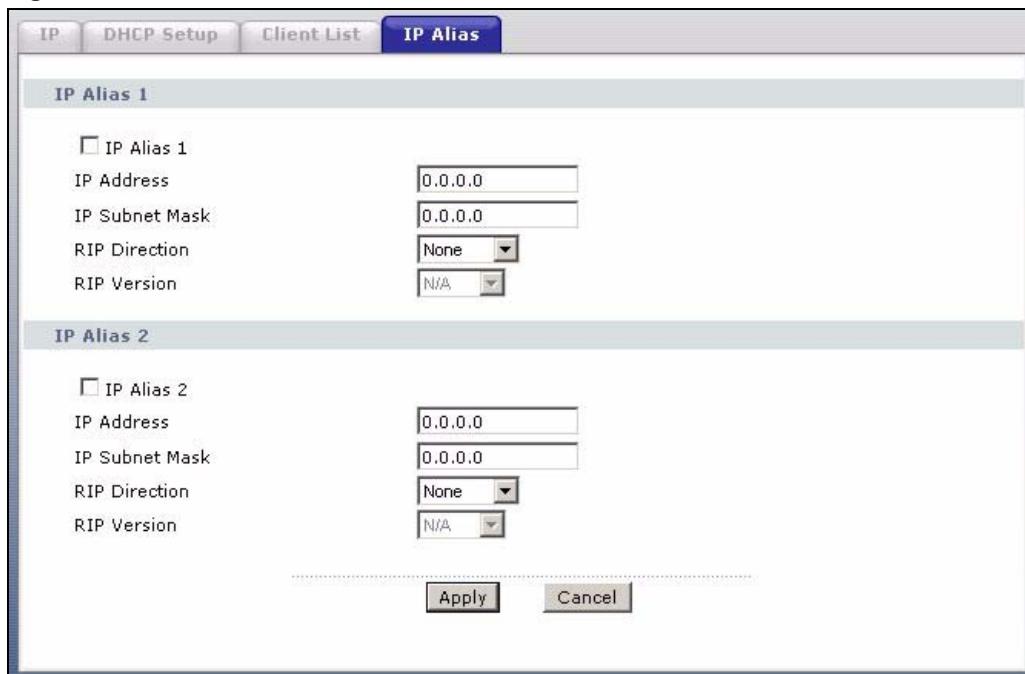
Note: Make sure that the subnets of the logical networks do not overlap.

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

Figure 64 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 65 LAN IP Alias

The following table describes the labels in this screen.

Table 37 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 to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 9

Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. See the appendices for more detailed information about wireless networks.

9.1 Wireless Network Overview

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the ZyXEL Device.
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

9.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

9.2.1 SSID

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

9.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.² A MAC address is usually written using twelve hexadecimal characters³; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

9.2.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

9.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

-
2. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
 3. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The types of encryption you can choose depend on the type of authentication. (See [Section 9.2.3 on page 132](#) for information about this.)

Table 38 Types of Encryption for Each Type of Authentication

	No Authentication	RADIUS Server
Weakest ↑ ↓ Strongest	No Security	
	Static WEP	
	WPA-PSK	WPA
	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

9.2.5 One-Touch Intelligent Security Technology (OTIST)

With ZyXEL's OTIST, you set up the SSID and WPA-PSK on the ZyXEL Device. Then, the ZyXEL Device transfers them to the devices in the wireless networks. As a result, you do not have to set up the SSID and encryption on every device in the wireless network.

The devices in the wireless network have to support OTIST, and they have to be in range of the ZyXEL Device when you activate it. See [Section 9.5 on page 142](#) for more details.

9.3 Wireless Performance Overview

The following sections introduce different ways to improve the performance of the wireless network.

9.3.1 Quality of Service (QoS)

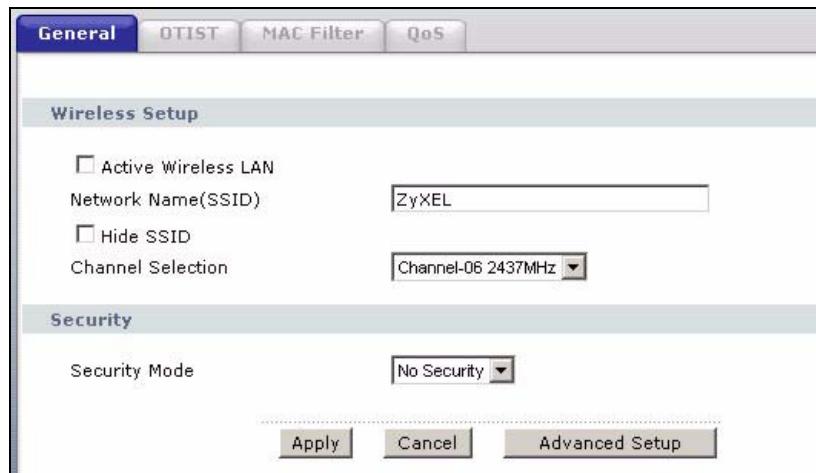
You can turn on Wi-Fi MultiMedia (WMM) QoS to improve the performance of voice and video applications in the wireless network. QoS gives high priority to voice and video, which makes them run more smoothly. Similarly, it gives low priority to many file downloads so that they do not reduce the quality of other applications.

9.4 General Wireless LAN Screen

Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or WEP settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

Click **Network > Wireless LAN** to open the **General** screen.

Figure 66 Wireless LAN: General



The following table describes the general wireless LAN labels in this screen. See the rest of this chapter for information on the labels that are available in this screen when you configure security.

If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

Table 39 Wireless LAN: General

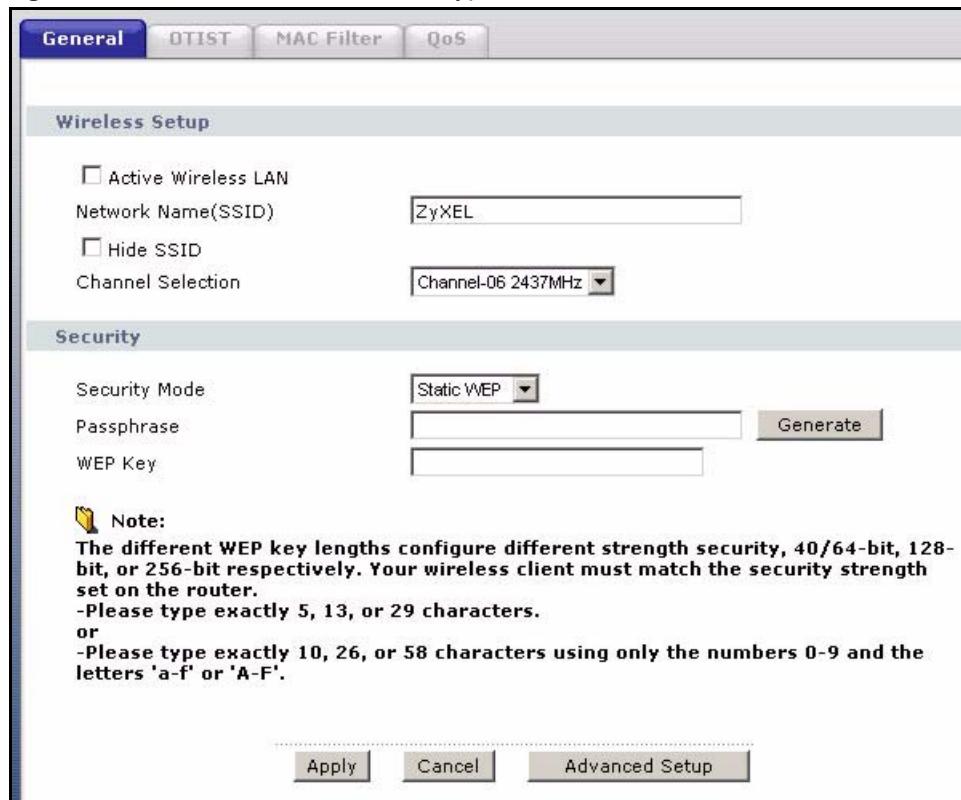
LABEL	DESCRIPTION
Active Wireless LAN	Select the check box to activate wireless LAN.
Network Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless client is associated. Wireless clients associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
Security Mode	Select No Security to allow wireless clients to communicate with the access points without any data encryption.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.
Advanced Setup	Click Advanced Setup to display the Wireless Advanced Setup screen and edit more details of your WLAN setup.

9.4.1 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless clients and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless clients and the access points must use the same WEP key.

Your ZyXEL Device allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Network > Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 67 Wireless: Static WEP Encryption

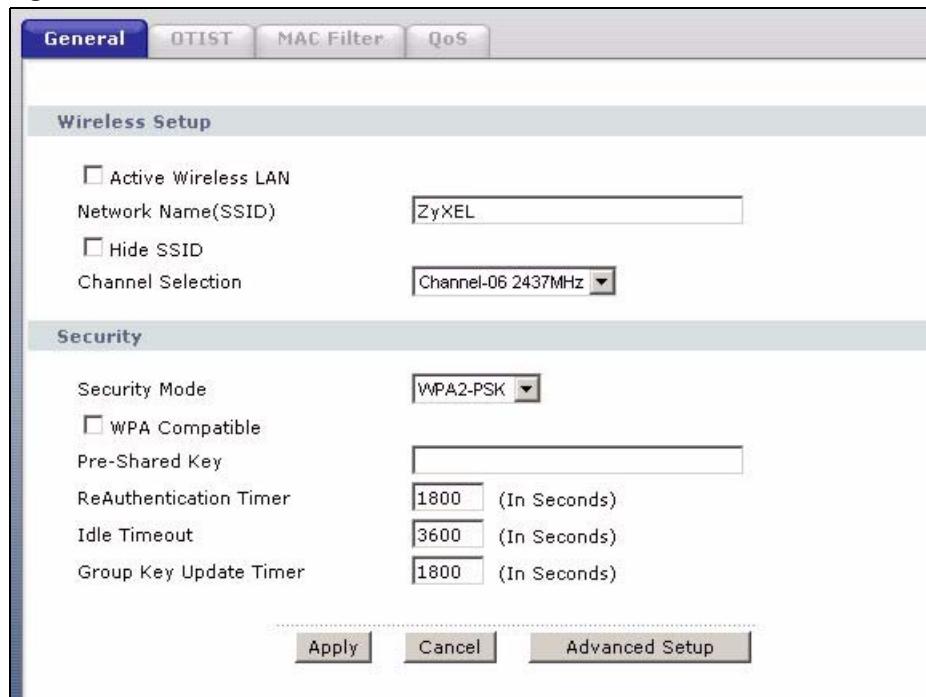
The following table describes the wireless LAN security labels in this screen.

Table 40 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose Static WEP from the drop-down list box.
Passphrase	Enter a Passphrase (up to 32 printable characters) and clicking Generate . The ZyXEL Device automatically generates a WEP key.
WEP Key	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless clients must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5, 13 or 29 characters (ASCII string) or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively.

9.4.2 WPA-PSK/WPA2-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 68 Wireless: WPA-PSK/WPA2-PSK

The following table describes the wireless LAN security labels in this screen.

Table 41 Wireless: WPA-PSK/WPA2-PSK

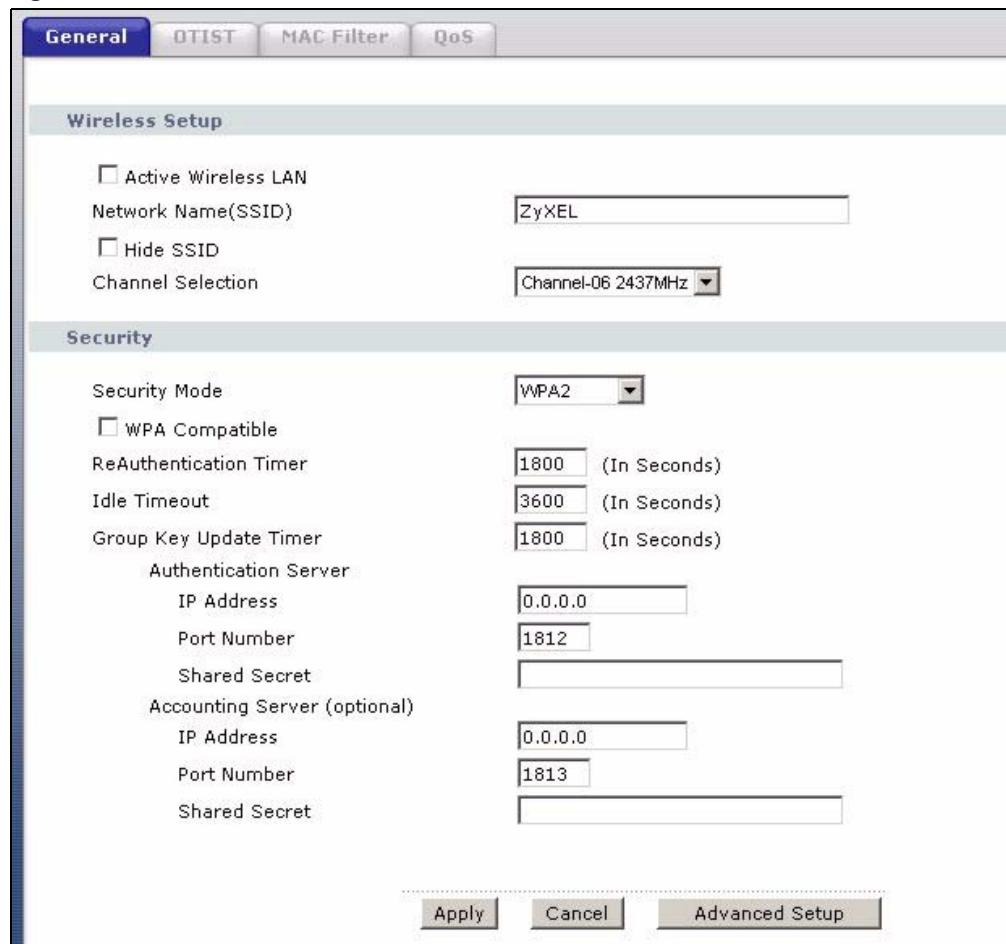
LABEL	DESCRIPTION
Security Mode	Choose WPA-PSK or WPA2-PSK from the drop-down list box.
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (In Seconds)	Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

Table 41 Wireless: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Idle Timeout (In Seconds)	The ZyXEL Device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again.
Group Key Update Timer (In Seconds)	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. The default is 1800 seconds (30 minutes).

9.4.3 WPA/WPA2

In order to configure and enable WPA/WPA2; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 69 Wireless: WPA/WPA2

The following table describes the wireless LAN security labels in this screen.

Table 42 Wireless: WPA/WPA2

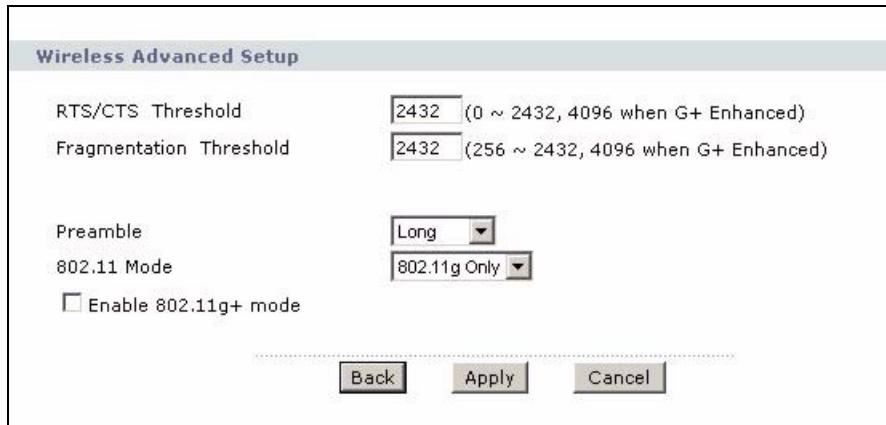
LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
ReAuthentication Timer (In Seconds)	Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (In Seconds)	The ZyXEL Device automatically disconnects a wireless client from the wired network after a period of inactivity. The wireless client needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

Table 42 Wireless: WPA/WPA2

LABEL	DESCRIPTION
Group Key Update Timer (In Seconds)	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. The default is 1800 seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server (optional)	
Active	Select Yes from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is 1813 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.

9.4.4 Wireless LAN Advanced Setup

To configure advanced wireless settings, click the **Advanced Setup** button in the **General** screen. The screen appears as shown.

Figure 70 Advanced

The following table describes the labels in this screen.

Table 43 Wireless LAN: Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Enter a value between 0 and 2432. If you select the Enable 802.11g+ mode checkbox, this field is grayed out and the ZyXEL Device uses 4096 automatically.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. If you select the Enable 802.11g+ mode checkbox, this field is grayed out and the ZyXEL Device uses 4096 automatically.
Preamble	Select Long preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks. Select Short preamble if you are sure the wireless adapters support it, and to provide more efficient communications. Select Dynamic to have the ZyXEL Device automatically use short preamble when wireless adapters support it, otherwise the ZyXEL Device uses long preamble.
802.11 Mode	Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Enable 802.11g+ mode	Select the Enable 802.11g+ mode checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the ZyXEL Device at higher transmission speeds. This permits the ZyXEL Device to transmit at a higher speed than the 802.11g Only mode.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.5 OTIST

In a wireless network, the wireless clients must have the same SSID and security settings as the access point (AP) or wireless router (we will refer to both as “AP” here) in order to associate with it. Traditionally this meant that you had to configure the settings on the AP and then manually configure the exact same settings on each wireless client.

OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP’s SSID and WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You can also choose to have OTIST generate a WPA-PSK key for you if you didn’t configure one manually.

Note: OTIST replaces the pre-configured wireless settings on the wireless clients.

9.5.1 Enabling OTIST

You must enable OTIST on both the AP and wireless client before you start transferring settings.

Note: The AP and wireless client(s) MUST use the same **Setup key**.

9.5.1.1 AP

You can enable OTIST using the **RESET** button or the web configurator.

9.5.1.1.1 Reset button

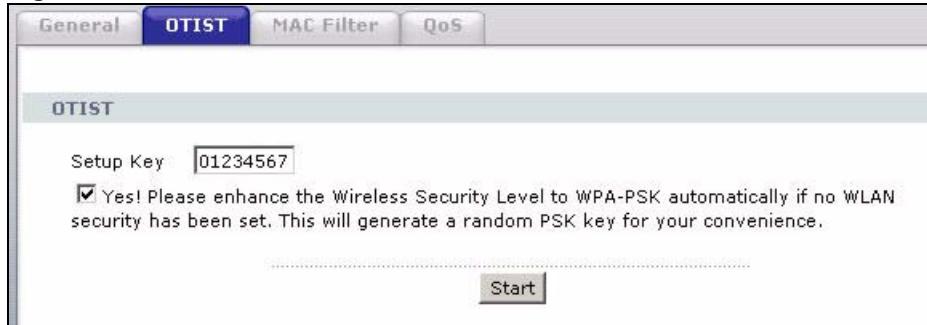
If you use the **RESET** button, the default (01234567) or previous saved (through the web configurator) **Setup key** is used to encrypt the settings that you want to transfer.

Hold in the **RESET** button for five seconds.

Note: If you hold in the **RESET** button too long, the device will reset to the factory defaults!

9.5.1.1.2 Web Configurator

Click the **Network > Wireless LAN > OTIST**. The following screen displays.

Figure 71 OTIST

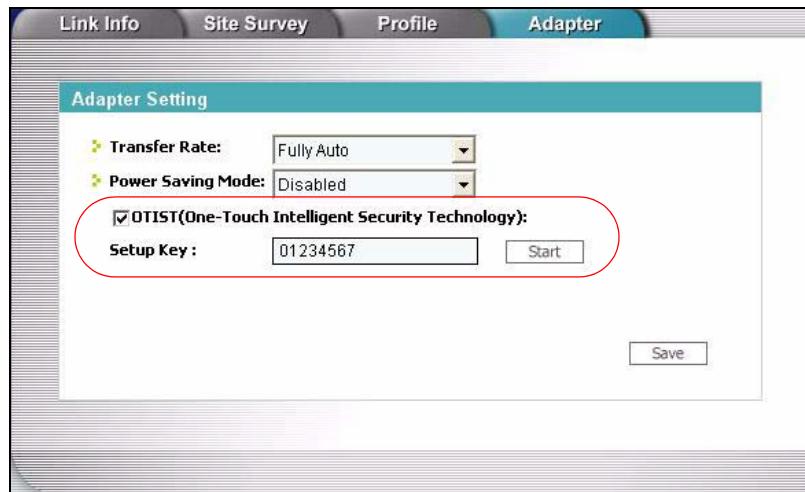
The following table describes the labels in this screen.

Table 44 OTIST

LABEL	DESCRIPTION
Setup Key	Type an OTIST Setup Key of exactly eight ASCII characters in length. The default OTIST setup key is "01234567". Note: If you change the OTIST setup key here, you must also make the same change on the wireless client(s).
Yes!	If you want OTIST to automatically generate a WPA-PSK, you must: Change your security to any security other than WPA-PSK in the Wireless LAN > General screen. Select the Yes! checkbox in the OTIST screen and click Start . The wireless screen displays an auto generated WPA-PSK and is now in WPA-PSK security mode. The WPA-PSK security settings are assigned to the wireless client when you start OTIST. Note: If you already have a WPA-PSK configured in the Wireless LAN > General screen, and you run OTIST with Yes! selected, OTIST will use the existing WPA-PSK.
Start	Click Start to encrypt the wireless security data using the setup key and have the Zyxel Device set the wireless client to use the same wireless settings as the Zyxel Device. You must also activate and start OTIST on the wireless client at the same time. The process takes three minutes to complete.

9.5.1.2 Wireless Client

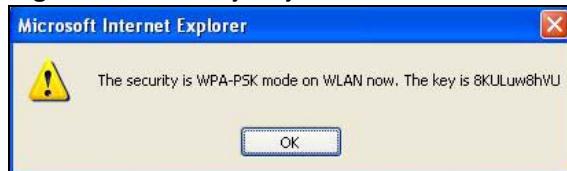
Start the Zyxel utility and click the **Adapter** tab. Select the **OTIST** check box, enter the same **Setup Key** as your AP and click **Save**.

Figure 72 Example Wireless Client OTIST Screen

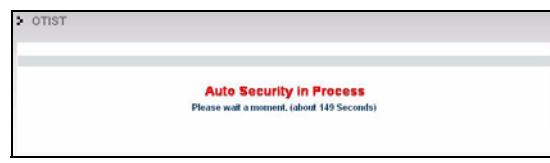
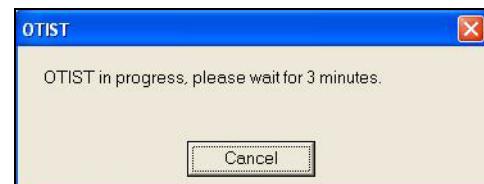
9.5.2 Starting OTIST

Note: You must click **Start** in the AP **OTIST** web configurator screen and in the wireless client(s) **Adapter** screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.

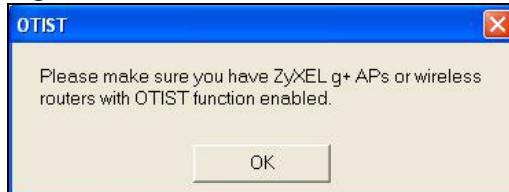
- 1 In the AP, a web configurator screen pops up showing you the security settings to transfer. You can use the key in this screen to set up WPA-PSK encryption manually for non-OTIST devices in the wireless network. After reviewing the settings, click **OK**.

Figure 73 Security Key

- 2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.

Figure 74 OTIST in Progress (AP)**Figure 75** OTIST in Progress (Client)

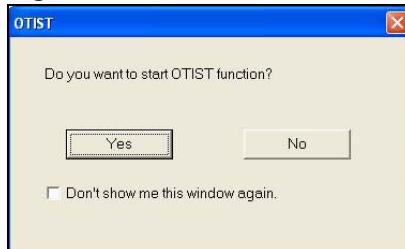
- 3 In the wireless client, you see this screen if it can't find an OTIST-enabled AP (with the same **Setup key**). Click **OK** to go back to the ZyXEL utility main screen.

Figure 76 No AP with OTIST Found

- If there is more than one OTIST-enabled AP within range, you see a screen asking you to select one AP to get settings from.

9.5.3 Notes on OTIST

- 1 If you enabled OTIST in the wireless client, you see this screen each time you start the utility. Click **Yes** for it to search for an OTIST-enabled AP.

Figure 77 Start OTIST?

- 2 If an OTIST-enabled wireless client loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless client search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)
- 3 When the wireless client finds an OTIST-enabled AP, you must still click **Start** in the AP **OTIST** web configurator screen or hold in the **RESET** button (for one to five seconds) for the AP to transfer settings.
- 4 If you change the SSID or the keys on the AP after using OTIST, you need to run OTIST again or enter them manually in the wireless client(s).
- 5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless client joins your wireless network, you need to run OTIST on the AP and ALL wireless clients again.

9.6 MAC Filter

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to up to 32 devices (**Allow**) or exclude up to 32 devices from accessing the ZyXEL Device (**Deny**). 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. You need to know the MAC address of the devices to configure this screen.

To change your ZyXEL Device's MAC filter settings, click **Network > Wireless LAN > MAC Filter**. The screen appears as shown.

Figure 78 MAC Address Filter

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00
9	00:00:00:00:00:00	10	00:00:00:00:00:00
11	00:00:00:00:00:00	12	00:00:00:00:00:00
13	00:00:00:00:00:00	14	00:00:00:00:00:00
15	00:00:00:00:00:00	16	00:00:00:00:00:00
17	00:00:00:00:00:00	18	00:00:00:00:00:00
19	00:00:00:00:00:00	20	00:00:00:00:00:00
21	00:00:00:00:00:00	22	00:00:00:00:00:00
23	00:00:00:00:00:00	24	00:00:00:00:00:00
25	00:00:00:00:00:00	26	00:00:00:00:00:00
27	00:00:00:00:00:00	28	00:00:00:00:00:00
29	00:00:00:00:00:00	30	00:00:00:00:00:00
31	00:00:00:00:00:00	32	00:00:00:00:00:00

Apply **Cancel**

The following table describes the labels in this menu.

Table 45 MAC Address Filter

LABEL	DESCRIPTION
Active MAC Filter	Select the check box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC Address table. Select Deny to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device. Select Allow to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless client that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

Table 45 MAC Address Filter

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.7 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services.

WMM is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

9.7.1 WMM QoS Example

When WMM QoS is not enabled, all traffic streams are given the same access throughput to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

When WMM QoS is enabled, the streams are prioritized according to the needs of the application. You can assign different priorities to different applications. This prevents reductions in data transmission for applications that are sensitive.

9.7.2 WMM QoS Priorities

The following table describes the priorities that you can apply to traffic that the ZyXEL Device sends to the wireless network.

Table 46 WMM QoS Priorities

PRIORITY LEVELS:	
Highest	Typically used for voice traffic or video that is especially sensitive to jitter (variations in delay). Use the highest priority to reduce latency for improved voice quality.
High	Typically used for video traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.
Mid	Typically used for traffic from applications or devices that lack QoS capabilities. Use mid priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
Low	This is typically used for non-critical “background” traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use low priority for applications that do not have strict latency and throughput requirements.

9.7.3 Services

See [Appendix G on page 407](#) for a list of commonly used services and port numbers.

9.8 QoS Screen

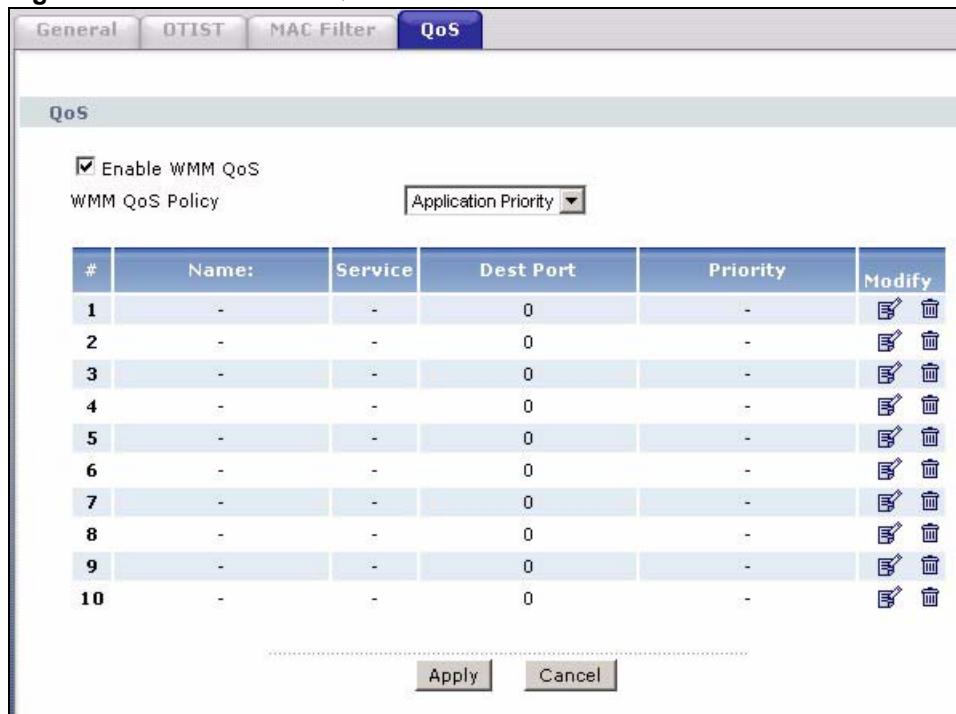
The QoS screen by default allows you to automatically give a service a priority level according to the ToS value in the IP header of the packets it sends.

9.8.1 ToS (Type of Service) and WMM QoS

ToS defines the DS (Differentiated Service) field in the IP packet header. The ToS value of outgoing packets is between 0 and 255. 0 is the lowest priority.

WMM QoS checks the ToS in the header of transmitted data packets. It gives the application a priority according to this number. If the ToS is not specified, then transmitted data is treated as normal or best-effort traffic.

Click **Network > Wireless LAN > QoS**. The following screen displays.

Figure 79 Wireless LAN: QoS

The following table describes the fields in this screen.

Table 47 Wireless LAN: QoS

LABEL	DESCRIPTION
QoS	
Enable WMM QoS	Select the check box to enable WMM QoS on the ZyXEL Device.
WMM QoS Policy	Select Default to have the ZyXEL Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. Select Application Priority from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either FTP , WWW , E-mail or a User Defined service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.
Priority	This field displays the WMM QoS priority for traffic bandwidth.
Modify	Click the Edit icon to open the Application Priority Configuration screen. Modify an existing application entry or create a application entry in the Application Priority Configuration screen. Click the Remove icon to delete an application entry.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.8.2 Application Priority Configuration

To edit a WMM QoS application entry, click the edit icon under **Modify**. The following screen displays.

Figure 80 Application Priority Configuration

The screenshot shows a window titled "Application Priority Configuration". It contains the following fields:

- Name: (empty input field)
- Service: (dropdown menu showing "E-Mail")
- Dest Port: (input field showing "25", with a note "(1~65535)")
- Priority: (dropdown menu showing "Highest")

At the bottom are two buttons: "Apply" and "Cancel".

The following table describes the fields in this screen.

Table 48 Application Priority Configuration

LABEL	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.
Service	<p>The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box.</p> <p>FTP File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.</p> <p>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</p> <p>WWW The World Wide Web 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.</p> <p>User-Defined User-defined services are user specific services configured using known ports and applications.</p>
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.

Table 48 Application Priority Configuration

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to return to the previous screen without saving your changes.

CHAPTER 10

Network Address Translation (NAT) Screens

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

10.1 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.

10.1.1 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 49 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.

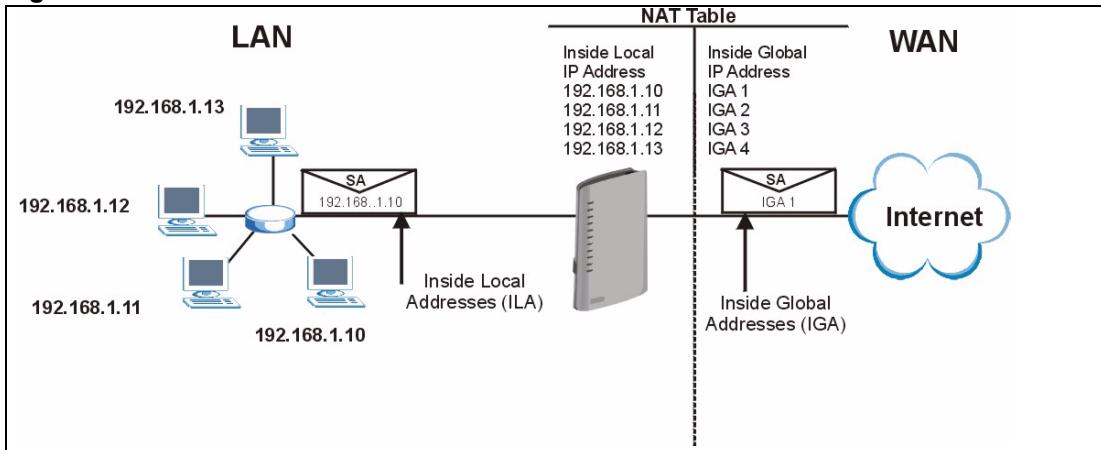
10.1.2 What NAT Does

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 50 on page 156](#)), 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)*.

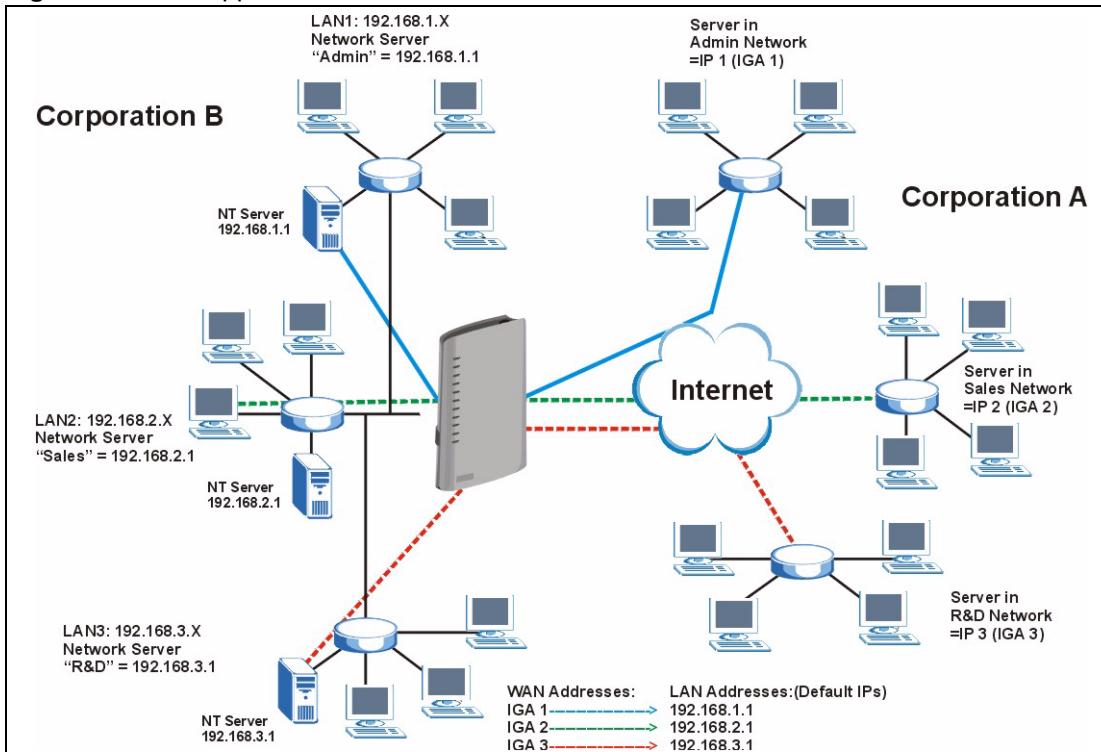
10.1.3 How NAT Works

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 81 How NAT Works

10.1.4 NAT Application

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

Figure 82 NAT Application With IP Alias

10.1.5 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 50 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1↔IGA1
Many-to-One (SUA/PAT)	ILA1↔IGA1 ILA2↔IGA1 ... ILA4↔IGA1
Many-to-Many Overload	ILA1↔IGA1 ILA2↔IGA2 ILA3↔IGA1 ILA4↔IGA2 ... ILA8↔IGA4
Many-to-Many No Overload	ILA1↔IGA1 ILA2↔IGA2 ILA3↔IGA3 ... ILA8↔IGA8
Server	Server 1 IP↔IGA1 Server 2 IP↔IGA1 Server 3 IP↔IGA1

10.2 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 50 on page 156](#).

- 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.

10.3 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 83 NAT General



The following table describes the labels in this screen.

Table 51 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 each client computer can establish through the ZyXEL Device. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.4 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.

10.4.1 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.

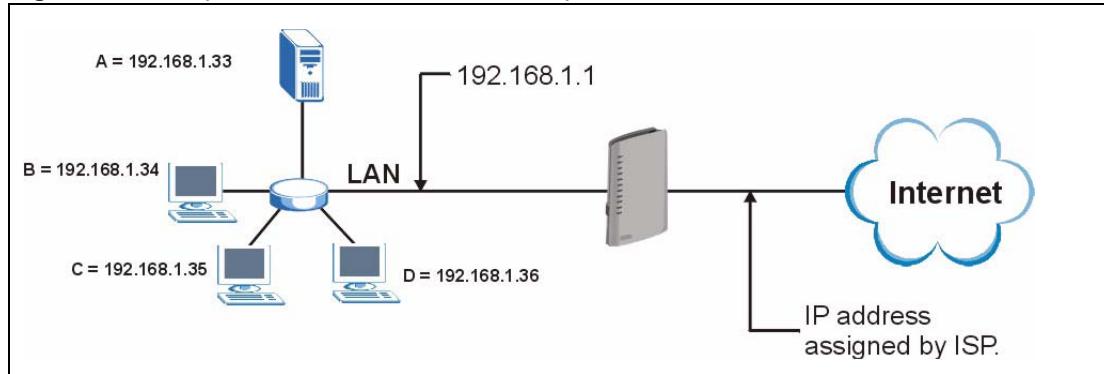
Note: If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

10.4.2 Port Forwarding: Services and Port Numbers

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network. See [Appendix G on page 407](#) for a list of commonly used services and port numbers.

10.4.3 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 84 Multiple Servers Behind NAT Example

10.5 Configuring Port Forwarding

Note: The **Port Forwarding** screen is available only when you select **SUA Only** in the **NAT > General** 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.

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

See [Table 177 on page 407](#) for port numbers commonly used for particular services.

Figure 85 Port Forwarding

#	Active	Service Name	Start Port	End Port	Server IP Address	Modify
1	<input checked="" type="checkbox"/>	WWW	80	80	172.23.15.23	

The following table describes the fields in this screen.

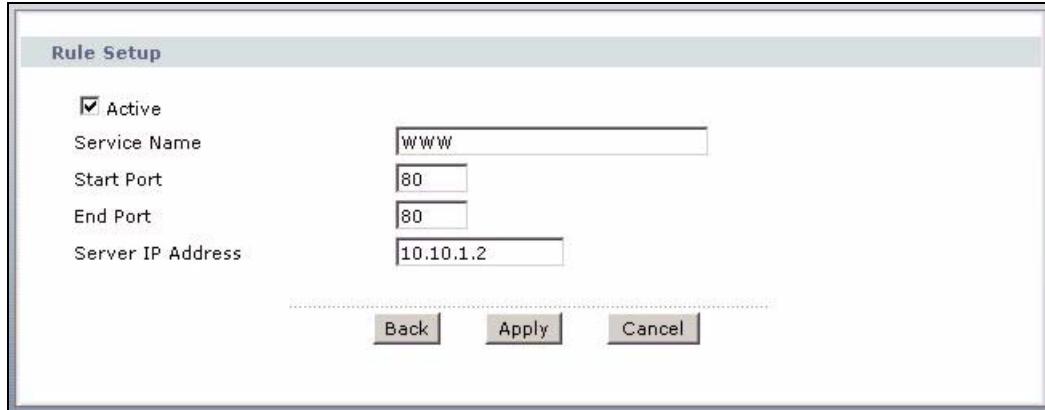
Table 52 Port Forwarding

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 to the ZyXEL Device.
Cancel	Click Cancel to return to the previous configuration.

10.5.1 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 86 Port Forwarding Rule Setup



The following table describes the fields in this screen.

Table 53 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 to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

10.6 Address Mapping

Note: The **Address Mapping** screen is available only when you select **Full Feature** in the **NAT > General** screen.

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

To change your ZyXEL Device's address mapping settings, click **Network > NAT > Address Mapping** to open the following screen.

Figure 87 Address Mapping Rules

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	-	-	-	-	-	
2	-	-	-	-	-	
3	-	-	-	-	-	
4	-	-	-	-	-	
5	-	-	-	-	-	
6	-	-	-	-	-	
7	-	-	-	-	-	
8	-	-	-	-	-	
9	-	-	-	-	-	
10	-	-	-	-	-	

The following table describes the fields in this screen.

Table 54 Address Mapping Rules

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

Table 54 Address Mapping Rules (continued)

LABEL	DESCRIPTION
Type	<p>1-1: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p>M-1: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p>M-M Ov (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p>MM No (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p>Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

10.6.1 Address Mapping Rule Edit

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

Figure 88 Edit Address Mapping Rule

The screenshot shows the 'Edit Address Mapping Rule1' configuration screen. It includes the following fields:

- Type: One-to-One
- Local Start IP: 0.0.0.0
- Local End IP: N/A
- Global Start IP: 0.0.0.0
- Global End IP: N/A
- Server Mapping Set: N/A (with a dropdown arrow and 'Edit Details' link)

At the bottom are three buttons: Back, Apply, and Cancel.

The following table describes the fields in this screen.

Table 55 Edit Address Mapping Rule

LABEL	DESCRIPTION
Type	<p>Choose the port mapping type from one of the following.</p> <p>One-to-One: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.</p> <p>Many-to-One: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p>Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p>Many-to-Many No Overload: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p>Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	<p>This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address.</p> <p>This field is N/A for One-to-One and Server mapping types.</p>
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Server Mapping Set	<p>Only available when Type is set to Server.</p> <p>Select a number from the drop-down menu to choose a port forwarding set.</p>
Edit Details	Click this link to go to the Port Forwarding screen to edit a port forwarding set that you have selected in the Server Mapping Set field.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 11

Voice

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

11.1 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.

11.2 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.

11.2.1 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.

11.2.1.1 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).

11.2.1.2 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.

11.2.2 SIP Call Progression

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

Table 56 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.

11.2.3 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.

11.2.3.1 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 89 SIP User Agent

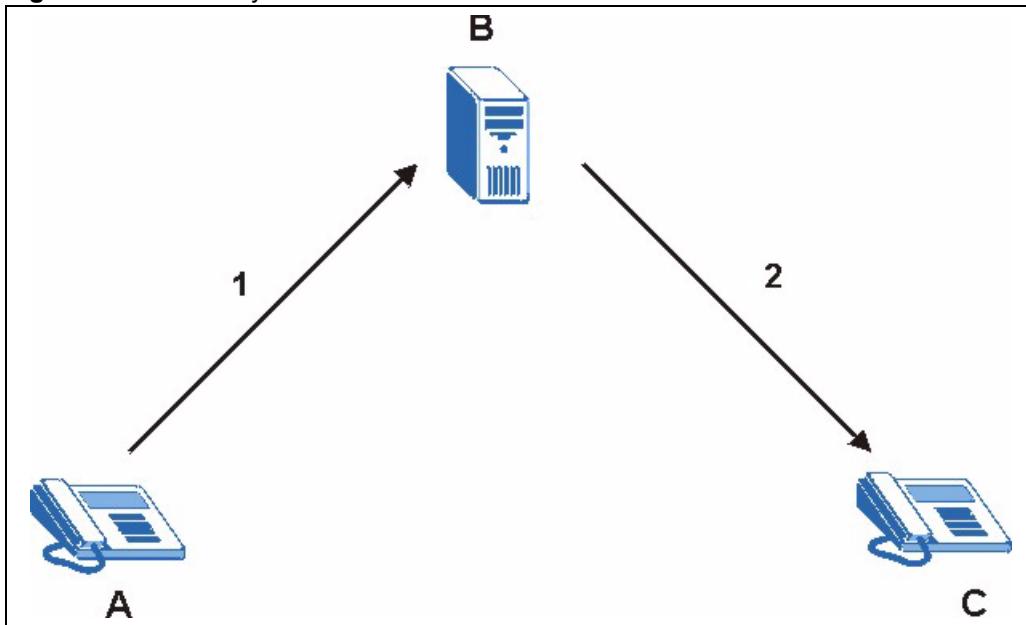


11.2.3.2 SIP Proxy Server

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.

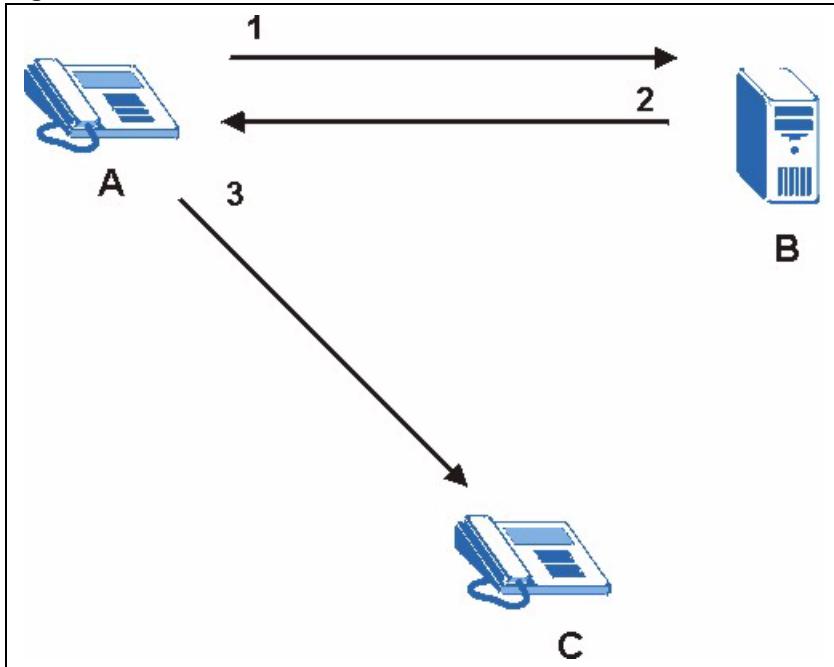
Figure 90 SIP Proxy Server

11.2.3.3 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.

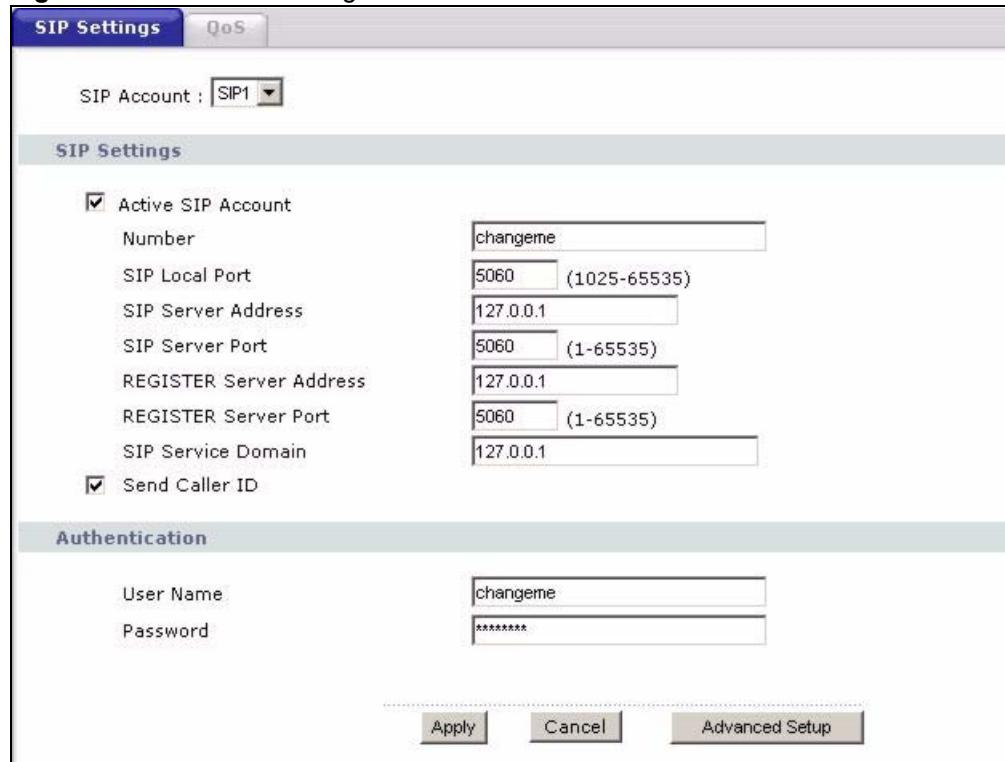
Figure 91 SIP Redirect Server

11.2.3.4 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.

11.3 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**.

Figure 92 SIP > SIP Settings

Each field is described in the following table.

Table 57 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 57 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.

11.3.1 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.

11.4 SIP ALG

The ZyXEL Device is a SIP Application Layer Gateway (ALG). A SIP ALG allows VoIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When a VoIP device behind the ZyXEL Device registers with the SIP register server, the ZyXEL Device translates the device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN with a VoIP device that is behind the ZyXEL Device.

11.5 Voice Coding

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

- **G.711** is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into bits. G.711 provides very good sound quality but requires 64kbps of bandwidth.
- **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.

11.6 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

11.7 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.

11.8 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 58 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.

11.8.0.1 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.
- 4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

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

11.8.0.2 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.

11.8.0.3 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.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

11.9 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 93 VoIP > SIP Settings > Advanced

SIP Account : SIP1		
SIP Server Settings		
URL Type	SIP	
Expiration Duration	3600 (20-65535) sec	
Register Re-send timer	180 (1-65535) sec	
Session Expires	180 (30-3600) sec	
Min-SE	30 (20-1800) sec	
RTP Port Range		
Start Port	50000 (1025-65535)	
End Port	65535 (1025-65535)	
Voice Compression		
Primary Compression Type	G.711A	
Secondary Compression Type	G.729	
Third Compression Type	None	
DTMF Mode	RFC 2833	
MWI (Message Waiting Indication)		
<input type="checkbox"/> Enable		
Expiration Time	1800 (1-65535) sec	
Fax Option		
<input checked="" type="radio"/> G.711 Fax Passthrough	<input type="radio"/> T.38 Fax Relay	
Call Forward		
Call Forward Table	Table 1	
Caller Ringing		
<input type="checkbox"/> Enable		
Caller Ringing Tone	Default	
On Hold		
<input type="checkbox"/> Enable		
On Hold Tone	Default	
.....		
<input type="button" value="Back"/>	<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>

Each field is described in the following table.

Table 59 VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
SIP Account	This field displays the SIP account you see in this screen.
SIP Server Settings	
URL Type	Select whether or not to include the SIP service domain name when the ZyXEL Device sends the SIP number. SIP - include the SIP service domain name TEL - do not include the SIP service domain name
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	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the Start Port and End Port fields. To enter a range of ports, enter the port number at the beginning of the range in the Start Port field and enter the port number at the end of the range in the End Port field.
Voice Compression	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). G.711A is typically used in Europe. G.711u is typically used in North America and Japan. In contrast, G.729 only requires 8 kbps. 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.
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 59 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>
MWI (Message Waiting Indication)	
Enable	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.
Expiration Time	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.
Fax Option	This field controls how the ZyXEL Device handles fax messages.
G.711 Fax Passthrough	Select this if the ZyXEL Device should use G.711 to send fax messages. The peer devices must also use G.711.
T.38 Fax Relay	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.
Call Forward	
Call Forward Table	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 .
Caller Ringing	
Enable	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 11.8 on page 172 for more information.
Caller Ringing Tone	Select the tone you want people to hear when they call you. You should setup these tones using IVR first. See Section 11.8 on page 172 for more information.
On Hold	
Enable	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 11.8 on page 172 for more information.
On Hold Tone	Select the tone you want people to hear when you put them on hold. You should setup these tones using IVR first. See Section 11.8 on page 172 for more information.
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.

11.10 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.

11.10.1 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.

11.10.2 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.

11.10.3 SIP QoS Screen

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

Note: You only need to configure this screen if your VoIP service provider or network administrator gave you ToS or VLAN settings.

Figure 94 SIP > QoS

Each field is described in the following table.

Table 60 SIP > QoS

LABEL	DESCRIPTION
SIP TOS Priority Setting	Enter the priority that your VoIP service provider or network administrator gave you 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 that your VoIP service provider or network administrator gave you for RTP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to RTP traffic that it transmits.
Voice VLAN ID	Select this if the ZyXEL Device has to be a member of a VLAN to communicate with the SIP server. Your LAN and gateway must be configured to use VLAN tags. Otherwise, clear this field. Ask your VoIP service provider or network administrator if you are not sure. Enter the VLAN ID provided by your VoIP service provider or network administrator in the field on the right.
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.

11.11 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.

11.12 PSTN Line

With the 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.

Note: When the ZyXEL Device does not have power, only the phone connected to the **PHONE 1** 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.

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).

11.13 ISDN Line

With ISDN line you can make and receive regular ISDN phone calls. Use a prefix number to make a regular call.

You can also use the **ISDN 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).

11.13.1 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.

11.13.2 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.

11.13.3 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.

11.14 Analog Phone Screen

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

Figure 95 Phone > Analog Phone

Each field is described in the following table.

Table 61 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.
PSTN Line	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, regardless of the settings you configure, only the phone connected to the PHONE 1 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.

11.15 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 96 Phone > Analog Phone > Advanced

The screenshot displays the 'Advanced Analog Phone Setup Screen' for 'Analog Phone 1'. It includes sections for 'Voice Volume Control' (Speaking Volume and Listening Volume dropdowns set to '-1 (Min.)'), 'Echo Cancellation' (G.168 Active checkbox), 'Dialing Interval Select' (value 3 and VAD Support checkbox), and a footer with 'Back', 'Apply', and 'Cancel' buttons.

Each field is described in the following table.

Table 62 Phone > Analog Phone > Advanced

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

Table 62 Phone > Analog Phone > Advanced

LABEL	DESCRIPTION
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.

11.16 ISDN Phone Screen

Use this screen to control which SIP accounts you use. To access this screen, click **VoIP > Phone > ISDN Phone**.

Figure 97 Phone > ISDN Phone

Each field is described in the following table.

Table 63 Phone > ISDN Phone

LABEL	DESCRIPTION
Outgoing Call Use	
SIP1	Select this if you want the ISDN 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 the ISDN 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.
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.

11.17 Common Phone Settings Screen

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

Figure 98 Phone > Common

Each field is described in the following table.

Table 64 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.

11.18 Supplementary Phone Services Overview (PSTN)

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

- Call Hold / Retrieve
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding (see [Section 11.23 on page 191](#))
- Three-Way Conference
- Internal Calls (see [Section 12.3 on page 197](#))
- Call Return

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.

11.18.1 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.

11.18.2 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 65 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.

11.18.2.1 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.

11.18.2.2 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**.

11.18.2.3 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.
- 3** After you hear the ring signal or the second party answers it, hang up the phone.

11.18.2.4 European Three-Way Conference

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

- 1** When you are on the phone talking to someone, place 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**.

11.18.2.5 European Call Return

To call the last number that called you, dial *66#. If you are using a phone connected to phone port 1, the ZyXEL Device will dial the last number to call phone port 1, and if you are using phone port 2 the ZyXEL Device will dial the last number to call phone port 2. The last caller must have been sending caller ID for you to return the call.

11.18.3 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 66 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		<p>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.</p> <p>Put a current call on hold to answer an incoming call.</p>
Flash	*98#	Transfer the call to another phone.

11.18.3.1 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.

11.18.3.2 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.

11.18.3.3 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.

11.18.3.4 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.

11.18.3.5 USA Call Return

To call the last number that called you, dial *66#. If you are using a phone connected to phone port 1, the ZyXEL Device will dial the number that last called phone port 1, and if you are using phone port 2 the ZyXEL Device will dial the number that last called phone port 2. The last caller must have been sending caller ID for you to return the call.

11.19 Supplementary Phone Services Overview (ISDN)

The ZyXEL Device supports several supplementary features for ISDN phones. You need to subscribe to these features from your ISDN phone service provider. How supplementary features are implemented may vary, so consult your ISDN phone service provider for details.

Features supported by the ZyXEL Device include:

- Call Hold / Retrieve

This feature allows you to temporarily stop a call without disconnecting it and resume it later.

- Making a Second Call

This feature allows you to temporarily stop a call and then make another outgoing call without disconnecting the first.

- Call Waiting

This feature allows you to temporarily stop a call and answer another incoming call without disconnecting the first.

- Three-way Conference

This feature allows you to set up a conversation with two people at the same time.

If you are making a conference call by ISDN phone using both SIP accounts, you must set them to have the same voice compression settings in the **VoIP > SIP Settings > Advanced screen**.

- Call Transfer

This feature allows you to switch an incoming call to another phone.

- Calling Line Identification Presentation (CLIP)

This feature allows the person you are calling to see your phone number if they are using a mobile phone or a phone with a digital screen.

- Calling Line Identification Restriction (CLIR)

This feature allows you to not send your phone number to the person you are calling, so they cannot see your number if they are using a mobile phone or a phone with a digital screen.

- Connected Line Identification Presentation (COLP)

This feature allows you to send your phone number to the person who is calling you.

- Connected Line Identification Restriction (COLR)

This feature allows you to not send your phone number to the person who is calling you. You might use this feature if your incoming calls are being forwarded to a number you wish to keep private.

- Advice of Charge During the Call (AOC-D)

This feature allows you to know the cost of your call while it is connected.

- Advice of Charge at the End of the Call (AOC-E)

This feature allows you to know the cost of your call once it is disconnected.

- Date / Time

This feature allows your ISDN phone to get its date and time settings from the ZyXEL Device.

11.20 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 99 VoIP > Phone > Region

Each field is described in the following table.

Table 67 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.

11.21 Speed Dial

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

11.21.1 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.

Note: You must still configure a SIP account on the ZyXEL Device in order to make a peer-to-peer VoIP call.

11.22 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 100 Phone Book > Speed Dial

The screenshot shows the 'Speed Dial' configuration page. At the top, there are tabs for 'Speed Dial' and 'Incoming Call Policy'. Below the tabs, the 'Speed Dial' section contains fields for 'Speed Dial' (set to '#01'), 'Number', 'Name:', and 'Type'. There are two radio buttons: 'Use Proxy' (selected) and 'Non-Proxy (Use IP or URL)'. A 'Add' button is located to the right of the 'Type' field. Below this is the 'Speed Dial Phone Book' section, which displays a table of 10 entries from #01 to #10. Each entry has columns for 'Speed Dial', 'Number', 'Name:', 'Destination', and 'Modify'. The 'Modify' column contains icons for edit and delete. At the bottom of the table are 'Clear' and 'Cancel' buttons.

Speed Dial	Number	Name:	Destination	Modify
#01				
#02				
#03				
#04				
#05				
#06				
#07				
#08				
#09				
#10				

Each field is described in the following table.

Table 68 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.
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.

Table 68 Phone Book > Speed Dial

LABEL	DESCRIPTION
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.

11.23 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 101 Phone Book > Incoming Call Policy

#	Activate	Incoming Call Number	Forward to Number	Condition
1	<input type="checkbox"/>			Unconditional
2	<input type="checkbox"/>			Unconditional
3	<input type="checkbox"/>			Unconditional
4	<input type="checkbox"/>			Unconditional
5	<input type="checkbox"/>			Unconditional
6	<input type="checkbox"/>			Unconditional
7	<input type="checkbox"/>			Unconditional
8	<input type="checkbox"/>			Unconditional
9	<input type="checkbox"/>			Unconditional
10	<input type="checkbox"/>			Unconditional

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 69 Phone Book > Incoming Call Policy

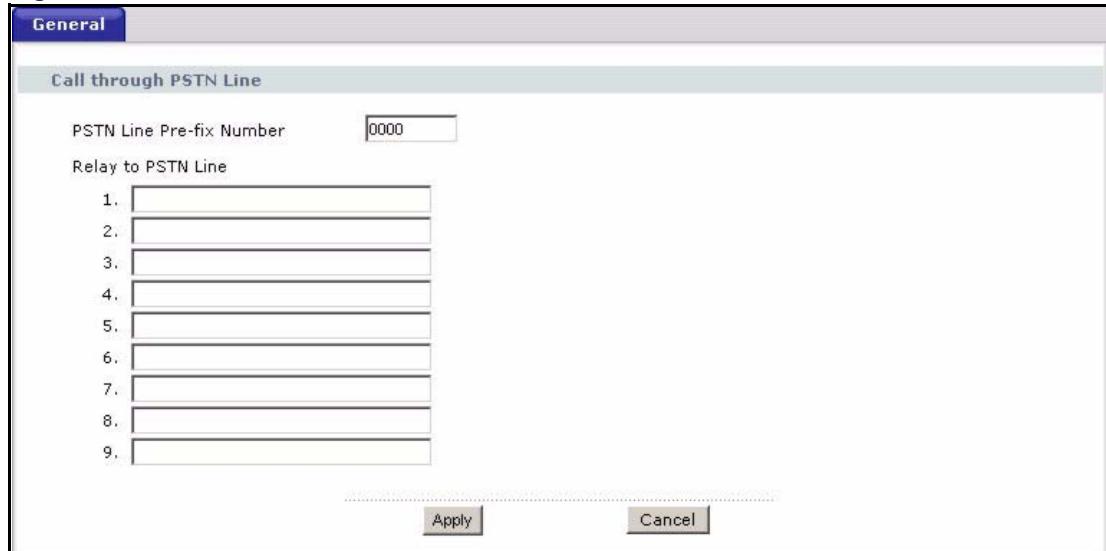
LABEL	DESCRIPTION
Table Number	Select the call-forwarding table you want to see in this screen. If you change this field, the screen automatically refreshes.
Forward to Number Setup	The ZyXEL Device checks these rules, in the order in which they appear, after it checks the rules in the Advanced Setup 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 69 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	Select the situations in which you want to forward incoming calls from the Incoming Call Number , or select an alternative action. Unconditional - The ZyXEL Device immediately forwards any calls from the Incoming Call Number to the Forward to Number . 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. 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 .) Block - The ZyXEL Device rejects calls from the Incoming Call Number . 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.
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.

11.24 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 102 PSTN Line > General

Each field is described in the following table.

Table 70 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.

11.25 ISDN Line Screen

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

Figure 103 ISDN Line > General

The screenshot shows a configuration interface for an ISDN line. The top bar is labeled "General". Below it, under the heading "Call through ISDN Line", there is a field for "ISDN Line Pre-fix Number" containing "0000". Below this is a section titled "Relay to ISDN Line" which includes a list of 9 fields numbered 1 to 9. At the bottom of the screen are two buttons: "Apply" and "Cancel".

Each field is described in the following table.

Table 71 ISDN Line > General

LABEL	DESCRIPTION
ISDN 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 ISDN 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 12

Phone Usage

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

12.1 Dialing a Telephone Number

The **PHONE** or **ISDN PHONE** light 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 11.21 on page 189](#)) 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.

12.2 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.

12.3 Internal Calls

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

12.4 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.

12.5 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 13

Firewalls

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

13.1 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 14.6 on page 216](#) to configure default firewall settings.

Refer to [Section 14.7 on page 218](#) to view firewall rules.

Refer to [Section 14.7.1 on page 219](#) to configure firewall rules.

Refer to [Section 14.7.2 on page 222](#) to configure a custom service.

Refer to [Section 14.10.3 on page 229](#) to configure firewall thresholds.

13.2 Types of Firewalls

There are three main types of firewalls:

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

13.2.1 Packet Filtering Firewalls

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

13.2.2 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.

13.2.3 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 13.5 on page 205](#) for more information on stateful inspection.

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

13.3 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.

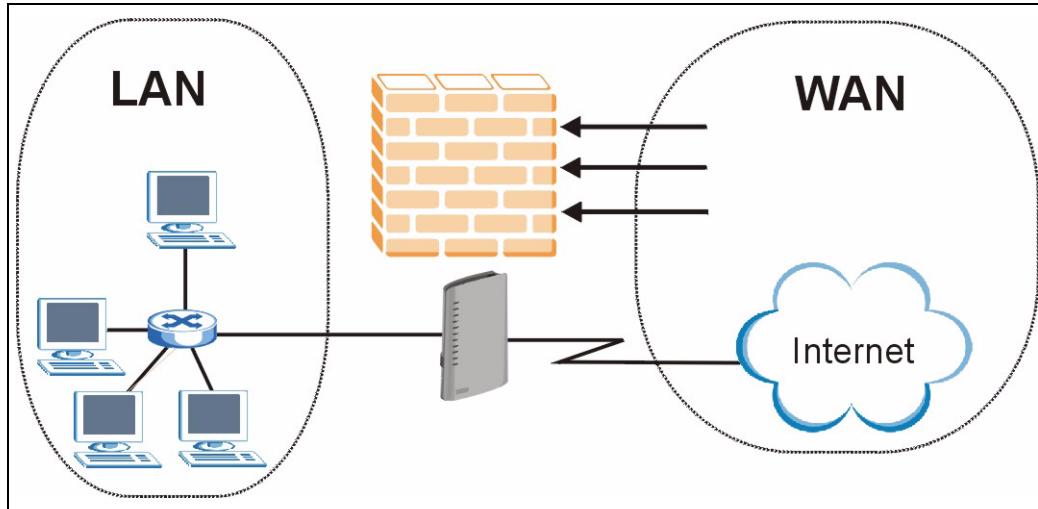
The ZyXEL Device has one DSL/ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

- 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.

13.3.1 Denial of Service Attacks

Figure 104 Firewall Application



13.4 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.

13.4.1 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:

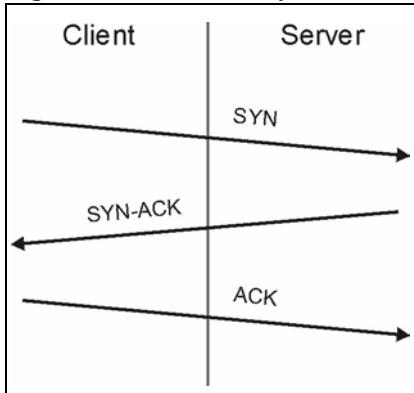
Table 72 Common IP Ports

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

13.4.2 Types of DoS Attacks

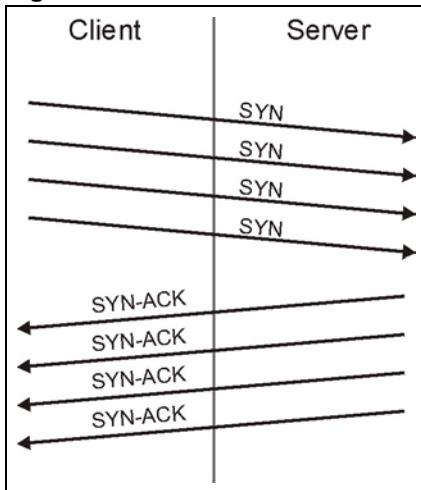
There are four types of DoS attacks:

- 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 105 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.

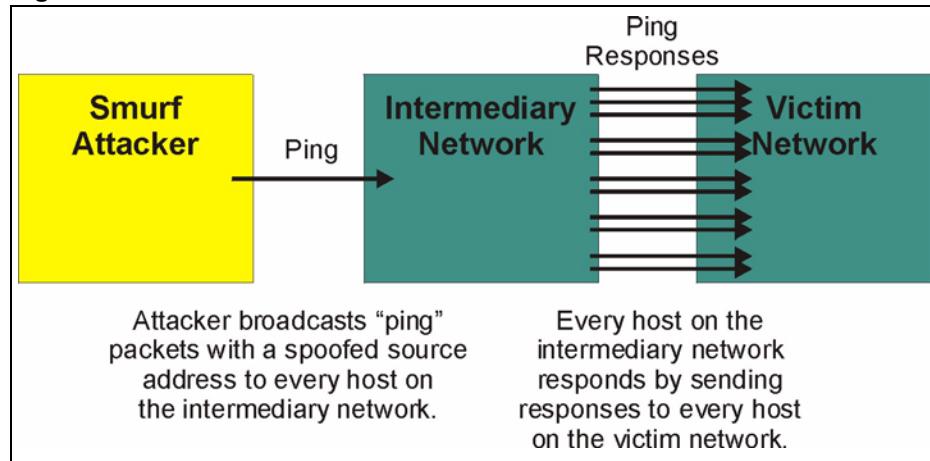
- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs 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 106 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 107 Smurf Attack

13.4.2.1 ICMP Vulnerability

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

Table 73 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

13.4.2.2 Illegal Commands (NetBIOS and SMTP)

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

Table 74 Legal NetBIOS Commands

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

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

Table 75 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

13.4.2.3 Traceroute

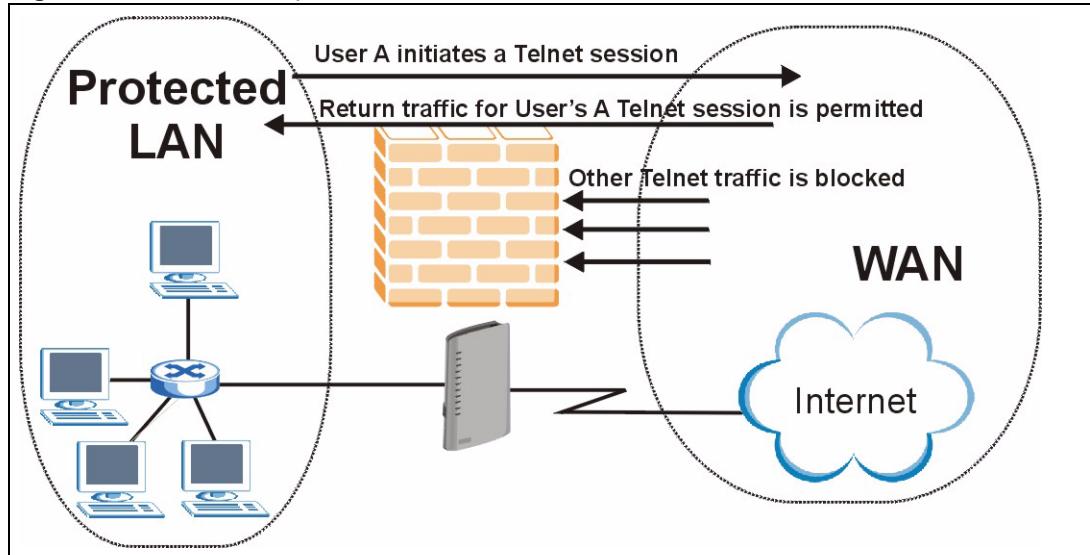
Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

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.

13.5 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 108 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.

13.5.1 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.

13.5.2 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).

13.5.3 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).

13.5.4 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.

13.5.5 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.

13.6 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.

13.6.1 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.

CHAPTER 14

Firewall Configuration

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

14.1 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.

14.2 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

Note: The LAN includes both the LAN port and the WLAN.

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.

14.3 Rule Logic Overview

Note: Study these points carefully before configuring rules.

14.3.1 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.

14.3.2 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.

14.3.3 Key Fields For Configuring Rules

14.3.3.1 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.

14.3.3.2 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 G on page 407](#) for a list of commonly used services and port numbers.

14.3.3.3 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?

14.3.3.4 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?

14.4 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 and WAN to WAN/ Router rules apply to packets coming in on the associated interface (LAN or WAN 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 policies apply in the same way to the WAN port.

14.4.1 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.

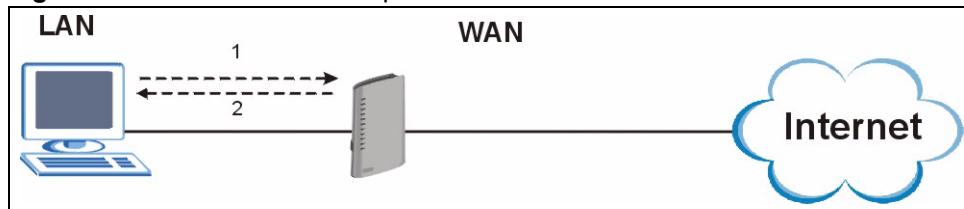
14.4.2 Alerts

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 114 on page 220](#)). 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 the chapter on logs for details.

14.5 Triangle Route

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 109 Ideal Firewall Setup



14.5.1 The “Triangle Route” Problem

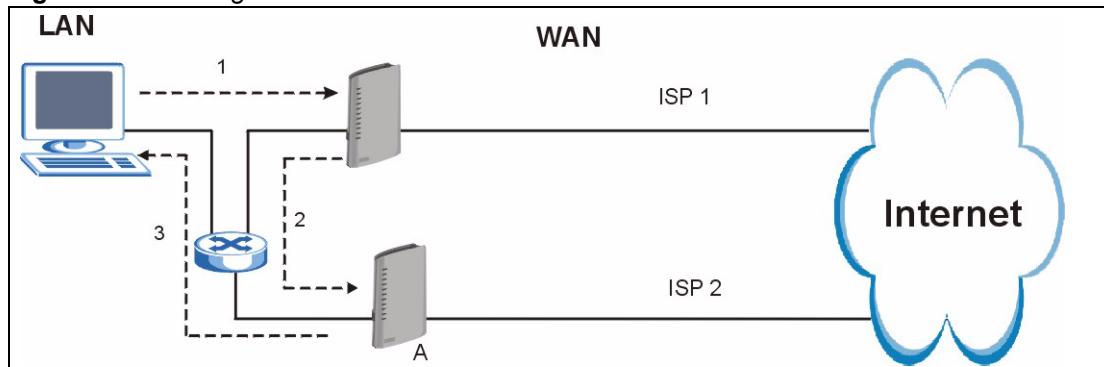
A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the ZyXEL Device's LAN IP address), the “triangle route” (also called asymmetrical 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 A 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 110 “Triangle Route” Problem

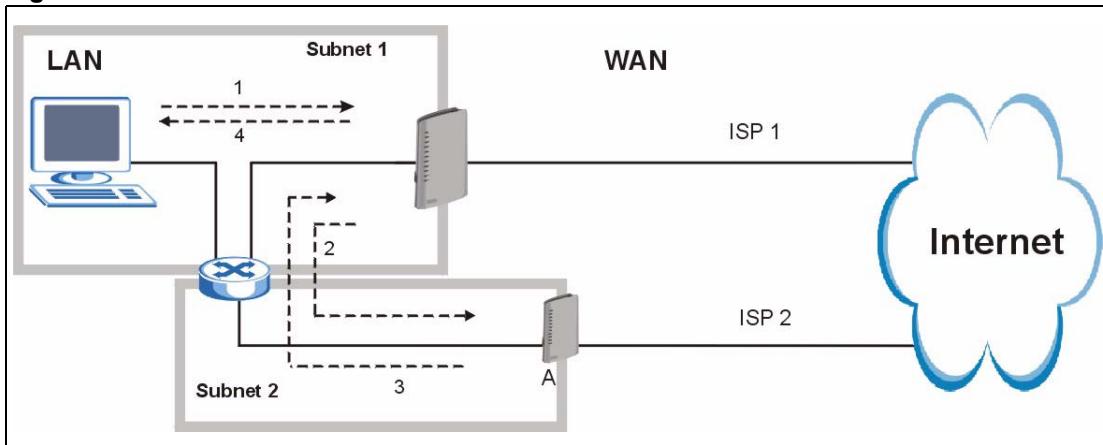


14.5.2 Solving the “Triangle Route” Problem

You can have the ZyXEL Device allow triangle route sessions. However this can allow traffic from the WAN to go directly to a LAN computer without passing through the ZyXEL Device and its firewall protection.

Another way to solve the triangle route problem is to use IP alias. 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 A in different subnets, all returning network traffic must pass through the ZyXEL Device to your LAN. The following steps describe such a scenario.

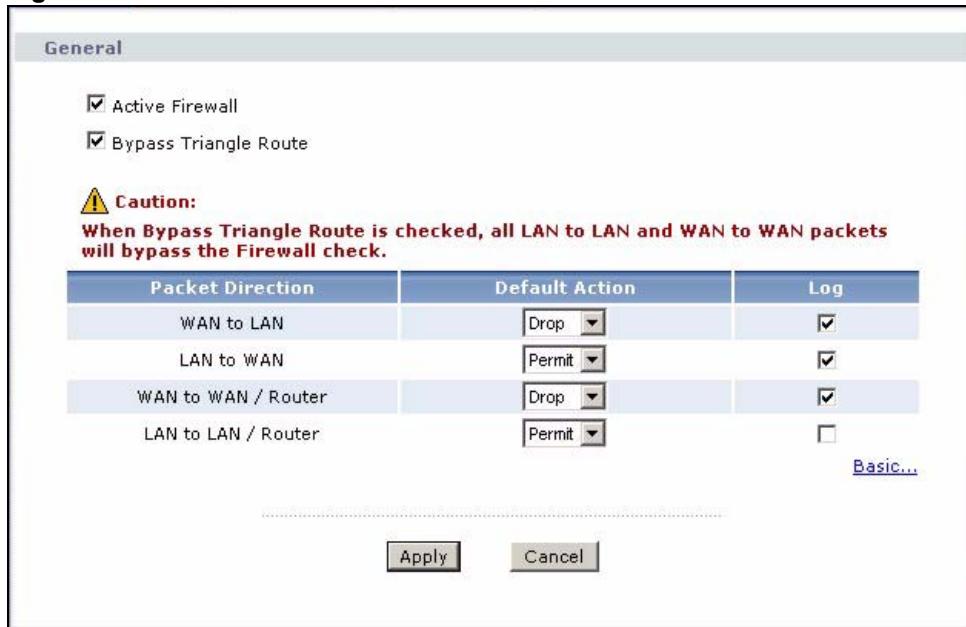
- 1** A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2** The ZyXEL Device reroutes the packet to Gateway A, which is in Subnet 2.
- 3** The reply from the WAN goes to the ZyXEL Device.
- 4** The ZyXEL Device then sends it to the computer on the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

Figure 111 IP Alias

14.6 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 13.1 on page 199](#) for more information.

Figure 112 Firewall: General

The following table describes the labels in this screen.

Table 76 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	Select this check box to have the ZyXEL Device firewall permit the use of triangle route topology on the network. Note: Allowing asymmetrical routes may let traffic from the WAN go directly to a LAN computer without passing through the router. See Section 14.5 on page 214 for more on triangle route topology and how to deal with this problem.
Packet Direction	This is the direction of travel of packets (LAN to LAN / Router , LAN to WAN , WAN to WAN / Router , WAN to LAN). 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.
Default Action	Use the drop-down list boxes to select the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules. 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.
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.

Table 76 Firewall: General (continued)

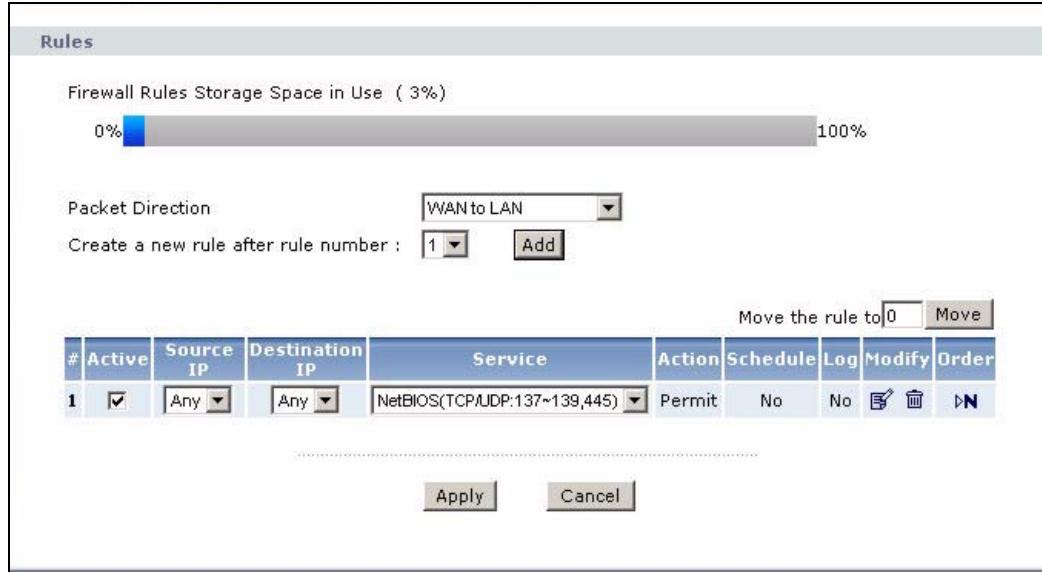
LABEL	DESCRIPTION
Expand...	Click this button to display more information.
Basic...	Click this button to display less information.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

14.7 Firewall Rules Summary

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

Refer to [Section 13.1 on page 199](#) 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 113 Firewall Rules

The following table describes the labels in this screen.

Table 77 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.

Table 77 Firewall Rules (continued)

LABEL	DESCRIPTION
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.
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).
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 to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

14.7.1 Configuring Firewall Rules

Refer to [Section 13.1 on page 199](#) 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 114 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
End IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0

Add >> Source Address List: Any

Edit << Delete

Destination 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

Add >> Destination Address List: Any

Edit << Delete

Service

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

Add >> Selected Services: Any(UDP), Any(TCP)

Remove Edit Customized Services

Schedule

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

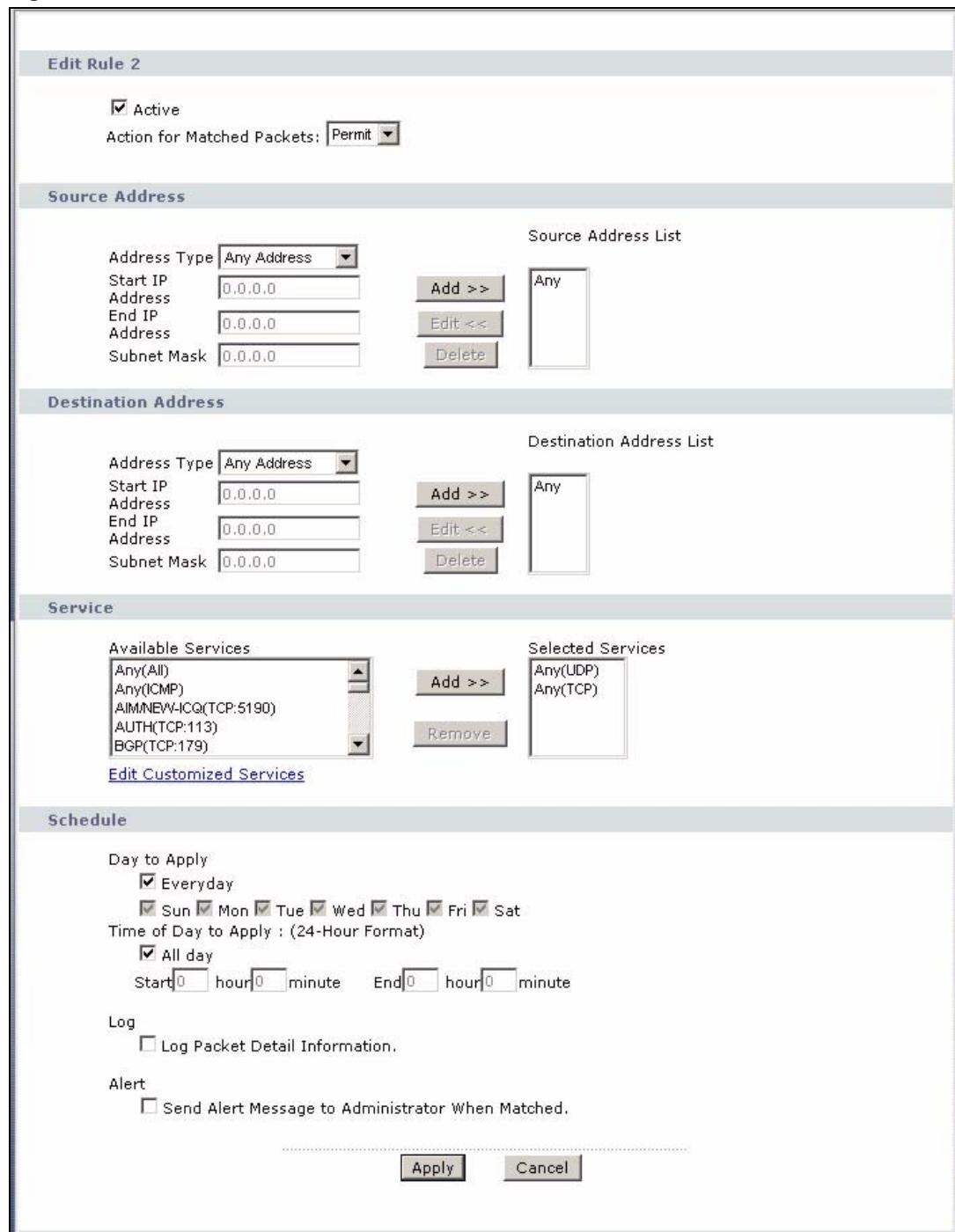
Time of Day to Apply : (24-Hour Format)
 All day
Start [0] hour [0] minute End [0] hour [0] minute

Log
 Log Packet Detail Information.

Alert
 Send Alert Message to Administrator When Matched.

.....

Apply Cancel



The following table describes the labels in this screen.

Table 78 Firewall: Edit Rule

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	<p>Use the drop-down list box to select what the firewall is to do with packets that match this rule.</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>
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	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.

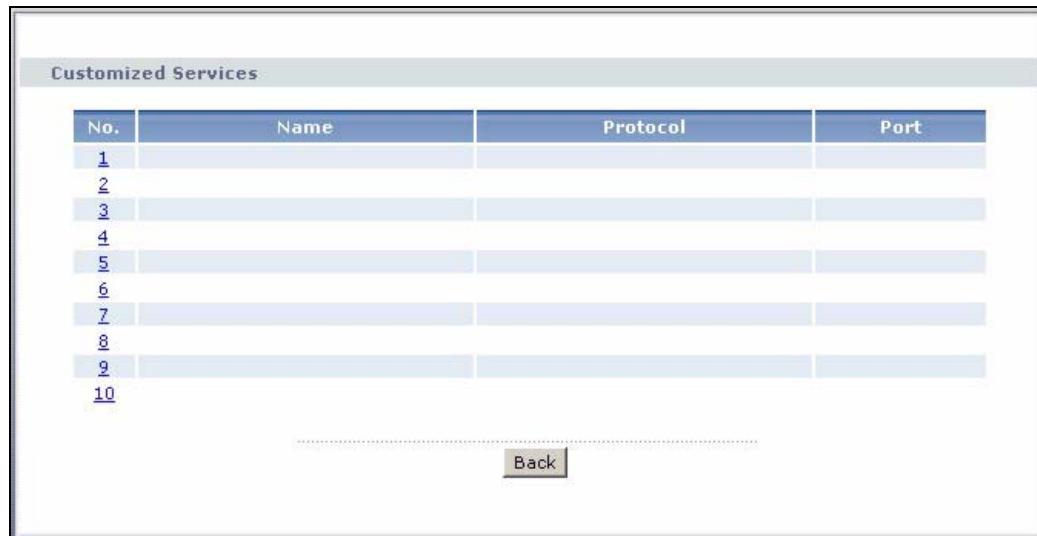
Table 78 Firewall: Edit Rule (continued)

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

14.7.2 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 G on page 407](#) for a list of commonly used services and port numbers. 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 13.1 on page 199](#) for more information.

Figure 115 Firewall: Customized Services

The following table describes the labels in this screen.

Table 79 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.

14.7.3 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 13.1 on page 199](#) for more information.

Figure 116 Firewall: Configure Customized Services

The following table describes the labels in this screen.

Table 80 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.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Delete	Click Delete to remove the current customized service entry.

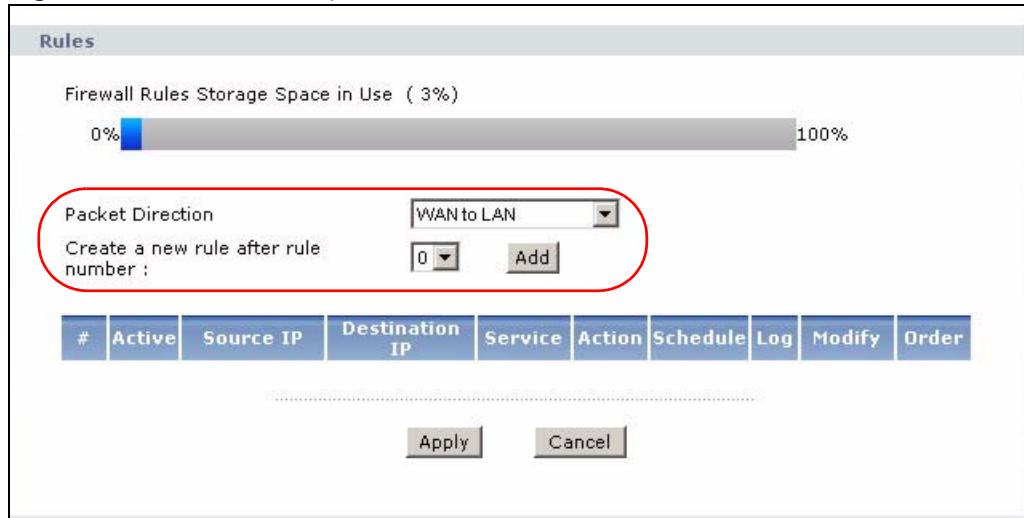
14.8 Example Firewall Rule

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

- 1 Click **Security > Firewall > Rules**.

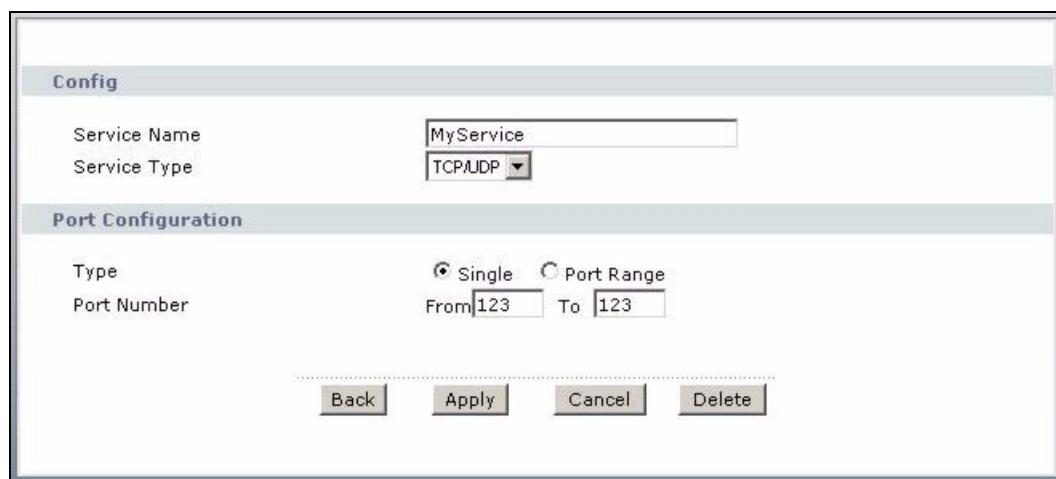
2 Select **WAN to LAN** in the **Packet Direction** field.

Figure 117 Firewall Example: Rules

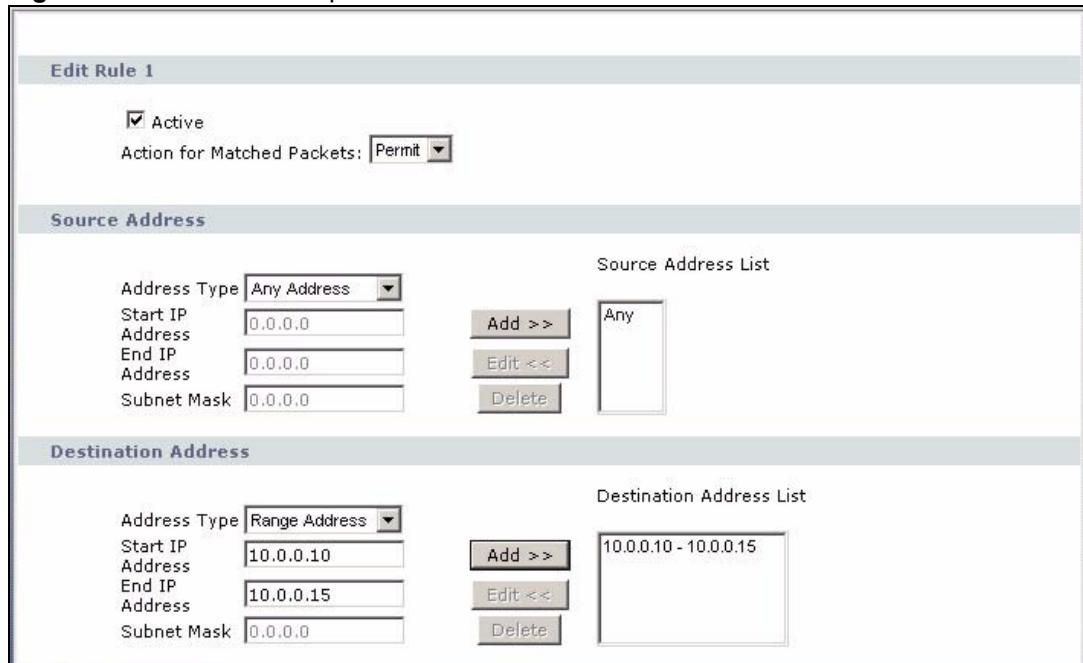


- 3** In the **Rules** screen, select the index number after which you want to add the rule. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
- 4** Click **Add** to display the firewall rule configuration screen.
- 5** In the **Edit 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 118 Edit Custom Port Example

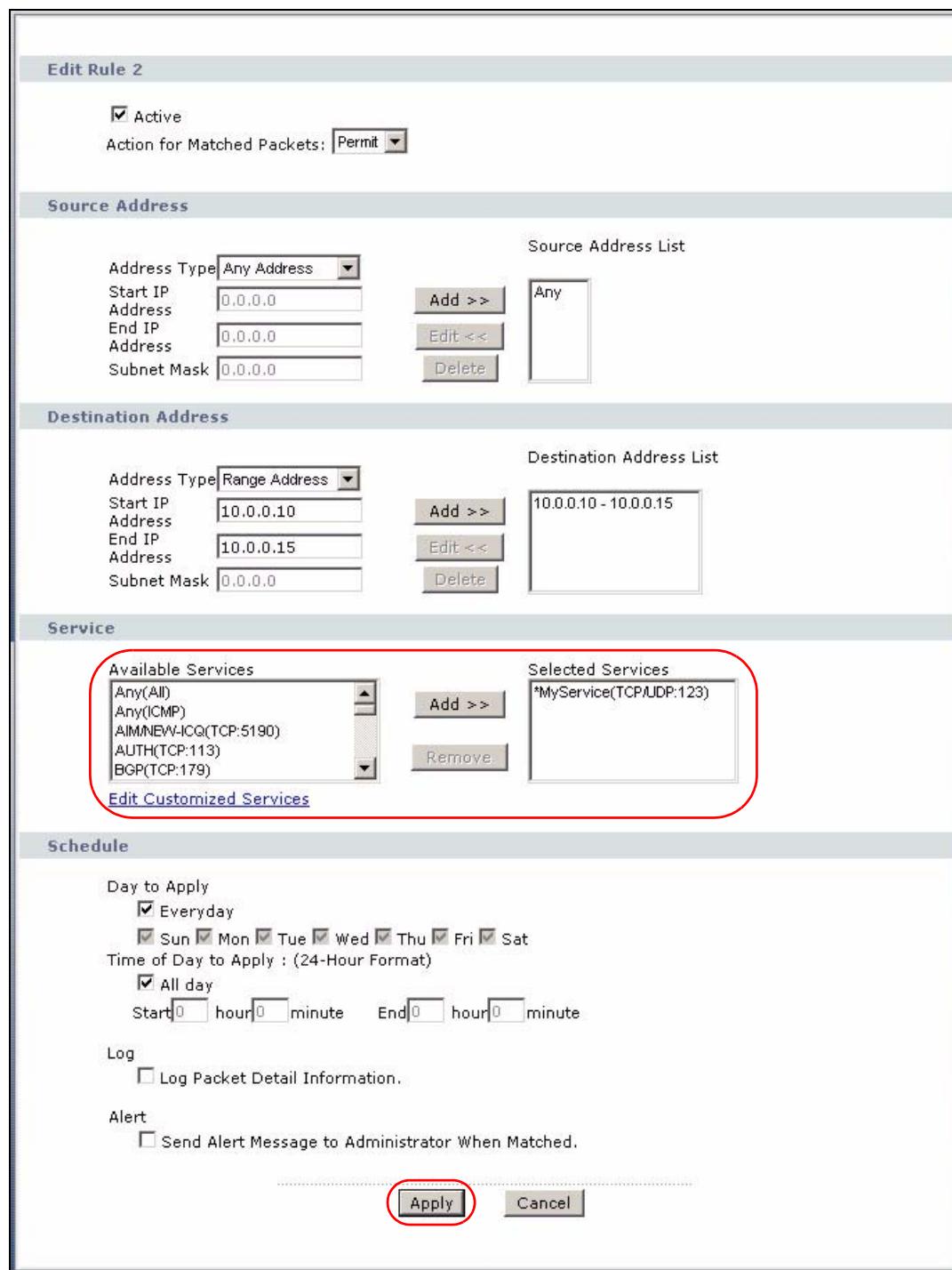


- 7** Select **Any** in the **Destination Address** box and then click **Delete**.
- 8** Configure the destination address screen as follows and click **Add**.

Figure 119 Firewall Example: Edit Rule: Destination Address

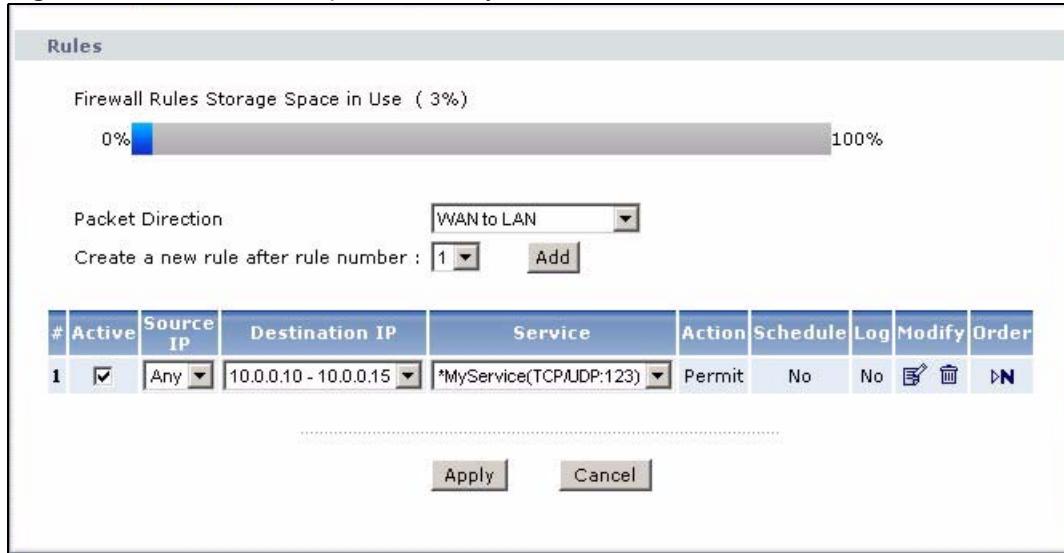
- 9** Use the **Add >>** and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.

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

Figure 120 Firewall Example: Edit Rule: Select Customized Services

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 121 Firewall Example: Rules: MyService

14.9 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see [Section 14.7.1 on page 219](#)) displays all predefined services that the ZyXEL Device already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “**(DNS)**”. **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Custom service ports may also be configured using the **Edit Customized Services** function discussed previously. See [Appendix G on page 407](#) for a list of commonly used services and port numbers.

14.10 Firewall Threshold

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 14.10.3 on page 229](#) to configure thresholds.

14.10.1 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.

14.10.2 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 105 on page 203](#)). 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.

14.10.2.1 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.

14.10.3 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 **Security > Firewall > Threshold** to bring up the next screen.

Figure 122 Firewall: Threshold

The screenshot shows the 'Firewall: Threshold' configuration page. It has two main sections: 'Denial of Service Thresholds' and 'Action taken when TCP Maximum Incomplete reached threshold'.

Denial of Service Thresholds:

Threshold Type	Value	Description
One Minute Low	80	(Sessions per Minute)
One Minute High	100	(Sessions per Minute)
Maximum Incomplete Low	80	(Sessions)
Maximum Incomplete High	100	(Sessions)
TCP Maximum Incomplete	10	(Sessions)

Action taken when TCP Maximum Incomplete reached threshold:

Delete the Oldest Half Open Session when New Connection Request Comes.
 Deny New Connection Request for Minutes(1~255)

Buttons at the bottom: Apply, Cancel.

The following table describes the labels in this screen.

Table 81 Firewall: Threshold

LABEL	DESCRIPTION
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.

Table 81 Firewall: Threshold (continued)

LABEL	DESCRIPTION
One Minute High	<p>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.</p> <p>For example, if you set the one minute high to 100, the ZyXEL Device starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.</p>
Maximum Incomplete Low	<p>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.</p>
Maximum Incomplete High	<p>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.</p> <p>For example, if you set the maximum incomplete high to 100, the ZyXEL Device starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.</p>
TCP Maximum Incomplete	<p>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.</p>
Action taken when the TCP Maximum Incomplete threshold is reached.	
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 to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 15

Content Filtering

This chapter covers how to configure content filtering.

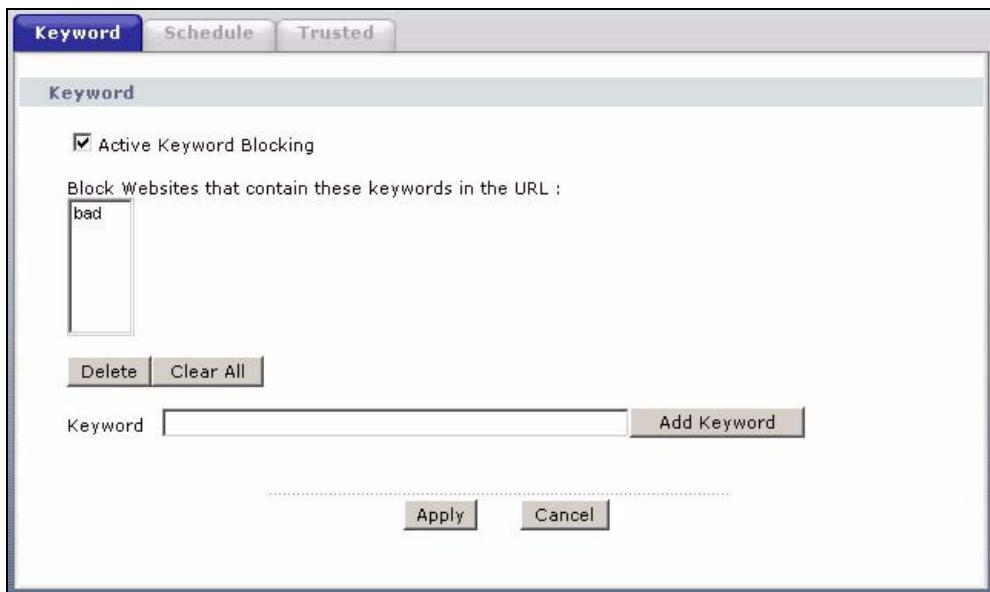
15.1 Content Filtering Overview

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.

15.2 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 123 Content Filter: Keyword

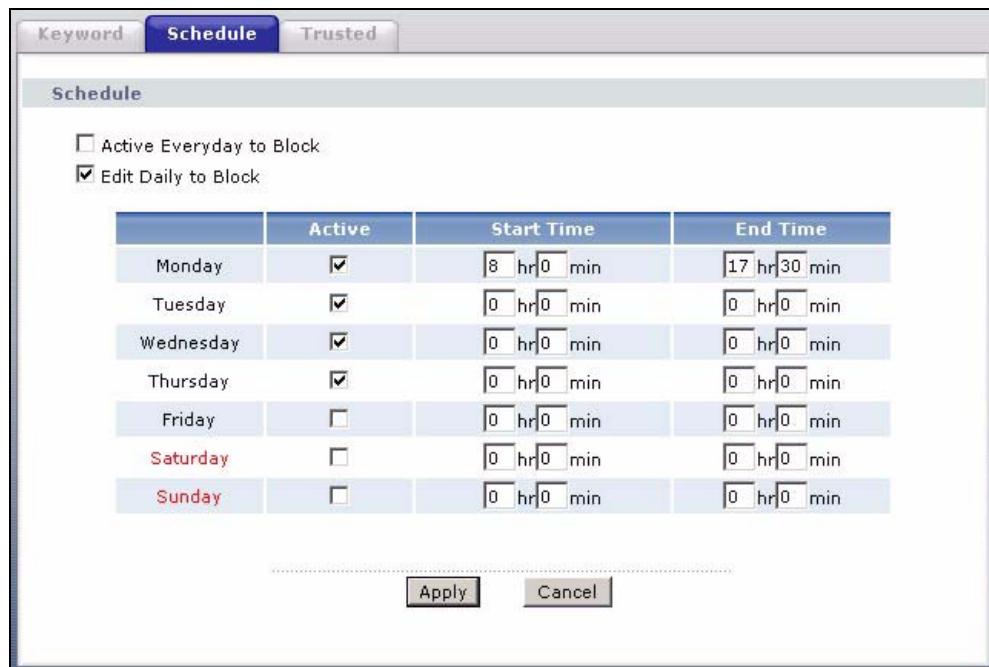
The following table describes the labels in this screen.

Table 82 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 to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

15.3 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 124 Content Filter: Schedule

The following table describes the labels in this screen.

Table 83 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 and which time of day you want the content filtering to be active.
Active	Select the check box to have the content filtering 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.

15.4 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 125 Content Filter: Trusted

The following table describes the labels in this screen.

Table 84 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 to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

CHAPTER 16

Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

16.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

16.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

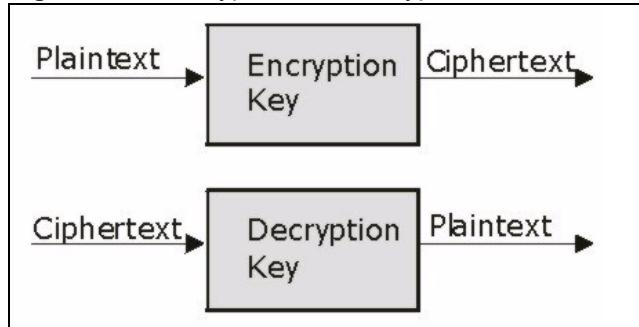
16.1.2 Security Association

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

16.1.3 Other Terminology

16.1.3.1 Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms "ciphertext" to plaintext. Decryption also requires a key.

Figure 126 Encryption and Decryption

16.1.3.2 Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

16.1.3.3 Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

16.1.3.4 Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

16.1.4 VPN Applications

The ZyXEL Device supports the following VPN applications.

- Linking Two or More Private Networks Together

Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- Accessing Network Resources When NAT Is Enabled

When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

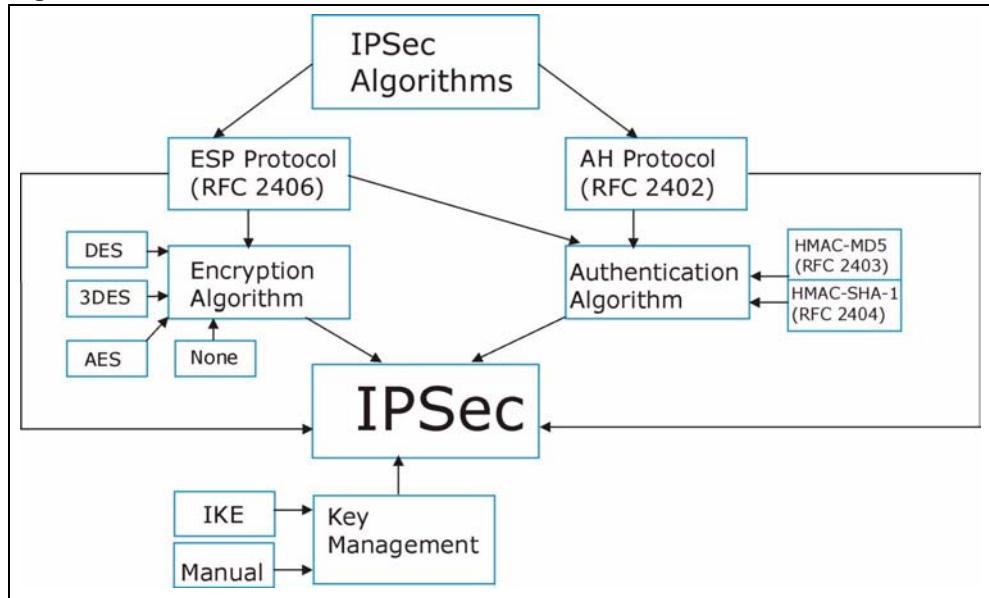
- Unsupported IP Applications

A VPN tunnel may be created to add support for unsupported emerging IP applications. See the chapter on *Getting to Know Your ZyXEL Device* for an example of a VPN application.

16.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 127 IPSec Architecture



16.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

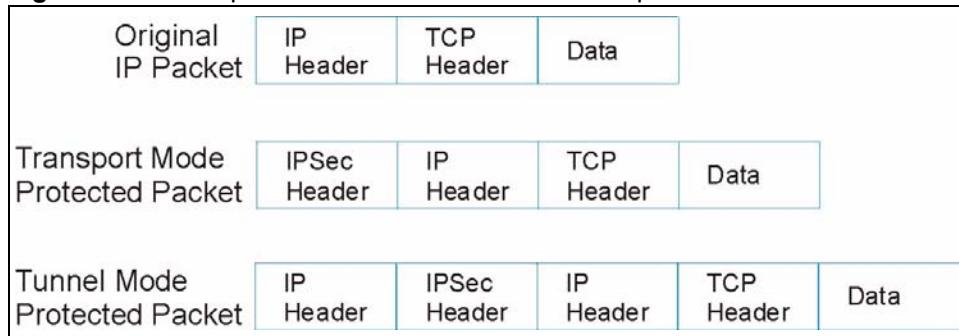
The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols. Please see [Section 17.2 on page 241](#) for more information.

16.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

16.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 128 Transport and Tunnel Mode IPSec Encapsulation

16.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP**, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

16.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header:** The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header:** The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

16.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyXEL Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 85 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

CHAPTER 17

VPN Screens

This chapter introduces the VPN screens. See the Logs chapter for information on viewing logs and the appendix for IPSec log descriptions.

17.1 VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

17.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

17.2.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

17.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 86 AH and ESP

	ESP	AH
ENCRYPTION	DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys ($3 \times 56 = 168$ bits), effectively doubling the strength of DES.	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
	Select NULL to set up a phase 2 tunnel without encryption.	
AUTHENTICATION	MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select MD5 for minimal security and SHA1 for maximum security.	

17.3 My IP Address

My IP Address is the WAN IP address of the ZyXEL Device. The ZyXEL Device has to rebuild the VPN tunnel if the My IP Address changes after setup.

The following applies if this field is configured as **0.0.0.0**:

- The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel.
- If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.

17.4 Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyXEL Device has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

17.4.1 Dynamic Secure Gateway Address

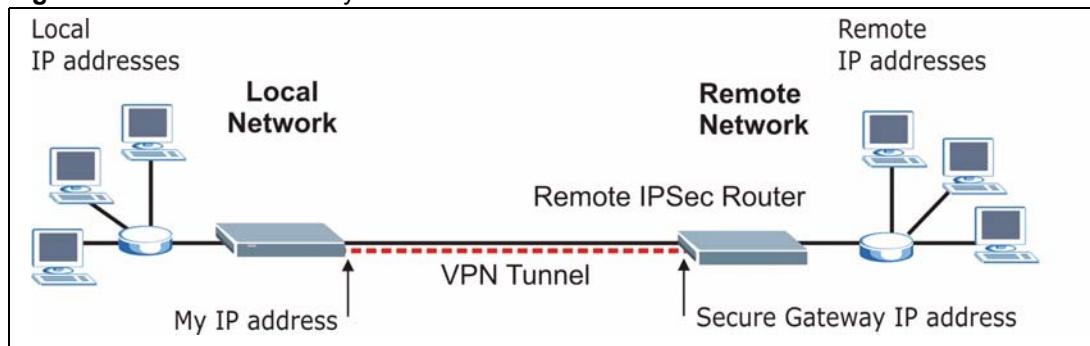
If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (see [Section 17.18 on page 264](#) for configuration examples).

The Secure Gateway IP Address may be configured as 0.0.0.0 only when using **IKE** key management and not **Manual** key management.

17.5 VPN Setup Screen

The following figure helps explain the main fields in the web configurator.

Figure 129 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **Security** and **VPN** to open the **VPN Setup** screen. This is a read-only menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by selecting an index number and then configuring its associated submenus.

Figure 130 VPN Setup

No.	Active	Name	Local Address	Remote Address	Encap.	IPSec Algorithm	Secure Gateway IP	Modify
1	-	-	-	-	...	
2	-	-	-	-	...	
3	-	-	-	-	...	
4	-	-	-	-	...	
5	-	-	-	-	...	
6	-	-	-	-	...	
7	-	-	-	-	...	
8	-	-	-	-	...	
9	-	-	-	-	...	
10	-	-	-	-	...	
11	-	-	-	-	...	
12	-	-	-	-	...	
13	-	-	-	-	...	
14	-	-	-	-	...	
15	-	-	-	-	...	
16	-	-	-	-	...	
17	-	-	-	-	...	
18	-	-	-	-	...	
19	-	-	-	-	...	
20	-	-	-	-	...	

Apply **Cancel**

The following table describes the fields in this screen.

Table 87 VPN Setup

LABEL	DESCRIPTION
No.	This is the VPN policy index number. Click a number to edit VPN policies.
Active	This field displays whether the VPN policy is active or not. A Yes signifies that this VPN policy is active. No signifies that this VPN policy is not active.
Name	This field displays the identification name for this VPN policy.
Local Address	<p>This is the IP address(es) of computer(s) on your local network behind your ZyXEL Device.</p> <p>The same (static) IP address is displayed twice when the Local Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Single.</p> <p>The beginning and ending (static) IP addresses, in a range of computers are displayed when the Local Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Range.</p> <p>A (static) IP address and a subnet mask are displayed when the Local Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Subnet.</p>

Table 87 VPN Setup

LABEL	DESCRIPTION
Remote Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays N/A when the Secure Gateway Address field displays 0.0.0.0 . In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the Remote Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Single . The beginning and ending (static) IP addresses, in a range of computers are displayed when the Remote Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Range . A (static) IP address and a subnet mask are displayed when the Remote Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Subnet .
Encap.	This field displays Tunnel or Transport mode (Tunnel is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyXEL Device processing requirements and communications latency (delay).
Secure Gateway IP	This is the static WAN IP address or URL of the remote IPSec router. This field displays 0.0.0.0 when you configure the Secure Gateway Address field in the VPN-IKE screen to 0.0.0.0 .
Modify	Click the Edit icon to go to the screen where you can edit the VPN configuration. Click the Remove icon to remove an existing VPN configuration.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

17.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL Device automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see [Section 17.12 on page 254](#) for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a ZyXEL Device-compatible keep alive feature enabled in order for this feature to work.

If the ZyXEL Device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyXEL Device because the ZyXEL Device never drops the tunnels that are already connected.

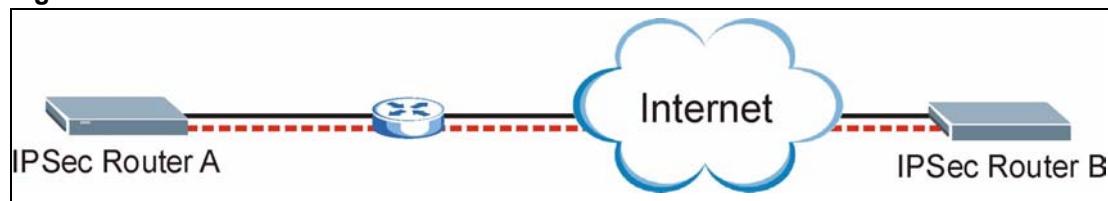
When there is outbound traffic with no inbound traffic, the ZyXEL Device automatically drops the tunnel after two minutes.

17.7 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the ZyXEL Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 131 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In [Figure 131 on page 246](#), when IPSec router A tries to establish an IKE SA, IPSec router B checks the UDP port 500 header, and IPSec routers A and B build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router A.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 88 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

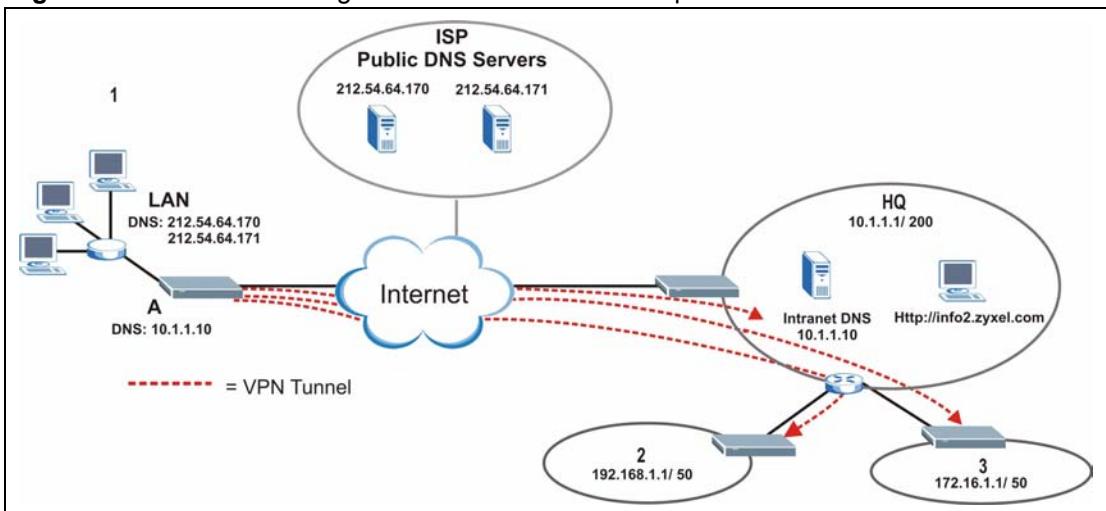
Y* - This is supported in the ZyXEL Device if you enable NAT traversal.

17.8 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote network.

The following figure depicts an example where three VPN tunnels are created from ZyXEL Device A; one to branch office 2, one to branch office 3 and another to headquarters. In order to access computers that use private domain names on the headquarters (HQ) network, the ZyXEL Device at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP.

Figure 132 VPN Host using Intranet DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

17.9 ID Type and Content

With aggressive negotiation mode (see [Section 17.12.1 on page 255](#)), the ZyXEL Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyXEL Device from IPSec routers with dynamic IP addresses (see [Section 17.18 on page 264](#) for a telecommuter configuration example).

Regardless of the ID type and content configuration, the ZyXEL Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see[Section 17.12.1 on page 255](#)), the ID type and content are encrypted to provide identity protection. In this case the ZyXEL Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL Device can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see[Section 17.13 on page 256](#)). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 89 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the ZyXEL Device automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyXEL Device.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyXEL Device.
	The domain name or e-mail address that you use in the Content field is used for identification purposes only and does not need to be a real domain name or e-mail address.

Table 90 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL Device automatically use the address in the Secure Gateway field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the Content field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the Secure Gateway Addr field below.

17.9.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two ZyXEL Devices in this example can complete negotiation and establish a VPN tunnel.

Table 91 Matching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two ZyXEL Devices in this example cannot complete their negotiation because ZyXEL Device B's **Local ID type** is **IP**, but ZyXEL Device A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 92 Mismatching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

17.10 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see [Section 17.12 on page 254](#) for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

17.11 Editing VPN Policies

Click an **Edit** icon in the [VPN Setup Screen](#) to edit VPN policies.

Figure 133 Edit VPN Policies

The following table describes the fields in this screen.

Table 93 Edit VPN Policies

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select either Yes or No from the drop-down list box. Select Yes to have the ZyXEL Device automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.

Table 93 Edit VPN Policies

LABEL	DESCRIPTION
NAT Traversal	This function is available if the VPN protocol is ESP . Select this check box if you want to set up a VPN tunnel when there are NAT routers between the ZyXEL Device and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
IPSec Key Mode	Select IKE or Manual from the drop-down list box. IKE provides more protection so it is generally recommended. Manual is a useful option for troubleshooting if you have problems using IKE key management.
Negotiation Mode	Select Main or Aggressive from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encapsulation Mode	Select Tunnel mode or Transport mode from the drop-down list box.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The ZyXEL Device assigns this additional DNS server to the ZyXEL Device's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0 , the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0 .
Local Address Type	Use the drop-down menu to choose Single , Range , or Subnet . Select Single for a single IP address. Select Range for a specific range of IP addresses. Select Subnet to specify IP addresses on a network by their subnet mask.
IP Address Start	When the Local Address Type field is configured to Single , enter a (static) IP address on the LAN behind your ZyXEL Device. When the Local Address Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the Local Address Type field is configured to Subnet , this is a (static) IP address on the LAN behind your ZyXEL Device.
End / Subnet Mask	When the Local Address Type field is configured to Single , this field is N/A. When the Local Address Type field is configured to Range , enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the Local Address Type field is configured to Subnet , this is a subnet mask on the LAN behind your ZyXEL Device.

Table 93 Edit VPN Policies

LABEL	DESCRIPTION
Remote	<p>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the Secure Gateway IP Address field is configured to 0.0.0.0. In this case only the remote IPSec router can initiate the VPN.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Remote Address Type	Use the drop-down menu to choose Single , Range , or Subnet . Select Single with a single IP address. Select Range for a specific range of IP addresses. Select Subnet to specify IP addresses on a network by their subnet mask.
IP Address Start	When the Remote Address Type field is configured to Single , enter a (static) IP address on the network behind the remote IPSec router. When the Remote Address Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Remote Address Type field is configured to Subnet , enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the Remote Address Type field is configured to Single , this field is N/A. When the Remote Address Type field is configured to Range , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Remote Address Type field is configured to Subnet , enter a subnet mask on the network behind the remote IPSec router.
Address Information	
Local ID Type	Select IP to identify this ZyXEL Device by its IP address. Select DNS to identify this ZyXEL Device by a domain name. Select E-mail to identify this ZyXEL Device by an e-mail address.
Content	<p>When you select IP in the Local ID Type field, type the IP address of your computer in the local Content field. The ZyXEL Device automatically uses the IP address in the My IP Address field (refer to the My IP Address field description) if you configure the local Content field to 0.0.0.0 or leave it blank.</p> <p>It is recommended that you type an IP address other than 0.0.0.0 in the local Content field or use the DNS or E-mail ID type in the following situations.</p> <p>When there is a NAT router between the two IPSec routers.</p> <p>When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.</p> <p>When you select DNS or E-mail in the Local ID Type field, type a domain name or e-mail address by which to identify this ZyXEL Device in the local Content field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.</p>
My IP Address	<p>Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>The following applies if this field is configured as 0.0.0.0:</p> <p>The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel.</p> <p>If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.</p>

Table 93 Edit VPN Policies

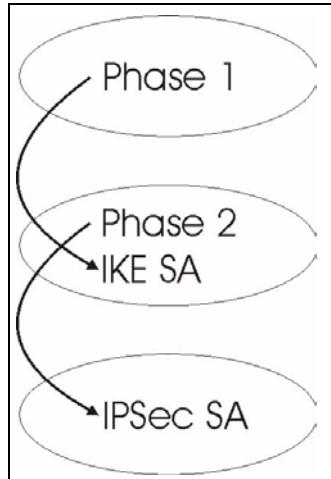
LABEL	DESCRIPTION
Peer ID Type	Select IP to identify the remote IPSec router by its IP address. Select DNS to identify the remote IPSec router by a domain name. Select E-mail to identify the remote IPSec router by an e-mail address.
Content	The configuration of the peer content depends on the peer ID type. For IP , type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the ZyXEL Device will use the address in the Secure Gateway Address field (refer to the Secure Gateway Address field description). For DNS or E-mail , type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than 0.0.0.0 or use the DNS or E-mail ID type in the following situations: When there is a NAT router between the two IPSec routers. When you want the ZyXEL Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the Key Management field must be set to IKE). In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0 , the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0 .
Security Protocol	
VPN Protocol	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH . If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below).
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.

Table 93 Edit VPN Policies

LABEL	DESCRIPTION
Encryption Algorithm	Select DES , 3DES , AES or NULL from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES . It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. AES is faster than 3DES . Select NULL to set up a tunnel without encryption. When you select NULL , you do not enter an encryption key.
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slower. Select MD5 for minimal security and SHA1 for maximum security.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.
Advanced Setup	Click Advanced Setup to configure more detailed settings of your IKE key management.

17.12 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 134 Two Phases to Set Up the IPSec SA

In phase 1 you must:

- Choose a negotiation mode.

- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see[Section 17.12.3 on page 256](#). Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyXEL Device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

17.12.1 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not known by the responder and both parties want to use pre-shared key authentication.

17.12.2 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

17.12.3 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyXEL Device. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

17.13 Configuring Advanced IKE Settings

Click **Advanced Setup** in the [Edit VPN Policies](#) screen to open this screen.

Figure 135 Advanced VPN Policies

VPN - IKE - Advanced Setup

Protocol	0
Enable Replay Detection	NO
Local Start Port	0 End 0
Remote Start Port	0 End 0

Phase1

Negotiation Mode	Main
Pre-Shared Key	(empty)
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time (Seconds)	28800
Key Group	DH1

Phase2

Active Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy (PFS)	NONE

Back Apply Cancel

The following table describes the fields in this screen.

Table 94 Advanced VPN Policies

LABEL	DESCRIPTION
VPN - IKE - Advanced Setup	
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select YES from the drop-down menu to enable replay detection, or select NO to disable it.
Local Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If Local Start Port is left at 0, End will also remain at 0.
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If Remote Start Port is left at 0, End will also remain at 0.
Phase 1	

Table 94 Advanced VPN Policies (continued)

LABEL	DESCRIPTION
Negotiation Mode	Select Main or Aggressive from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62-character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select DES , 3DES or AES from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES . It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. AES is faster than 3DES .
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slower. Select MD5 for minimal security and SHA1 for maximum security.
SA Life Time (Seconds)	Define the length of time before an IPSec SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Use the drop-down list box to choose from ESP or AH .
Encryption Algorithm	This field is available when you select ESP in the Active Protocol field. Select DES , 3DES , AES or NULL from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES . It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. AES is faster than 3DES . Select NULL to set up a tunnel without encryption. When you select NULL , you do not enter an encryption key.

Table 94 Advanced VPN Policies (continued)

LABEL	DESCRIPTION
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA1 for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select Tunnel mode or Transport mode from the drop-down list box.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (NONE) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose DH1 or DH2 from the drop-down list box to enable PFS. DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes to the ZyXEL Device and return to the VPN-IKE screen.
Cancel	Click Cancel to return to the VPN-IKE screen without saving your changes.

17.14 Manual Key Setup

Manual key management is useful if you have problems with **IKE** key management.

17.14.1 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

17.15 Configuring Manual Key

You only configure **VPN Manual Key** when you select **Manual** in the **IPSec Key Mode** field on the **VPN IKE** screen. This is the **VPN Manual Key** screen as shown next.

Figure 136 VPN: Manual Key

The following table describes the fields in this screen.

Table 95 VPN: Manual Key

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
IPSec Key Mode	Select IKE or Manual from the drop-down list box. Manual is a useful option for troubleshooting if you have problems using IKE key management.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Encapsulation Mode	Select Tunnel mode or Transport mode from the drop-down list box.

Table 95 VPN: Manual Key (continued)

LABEL	DESCRIPTION
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The ZyXEL Device assigns this additional DNS server to the ZyXEL Device's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose Single , Range , or Subnet . Select Single for a single IP address. Select Range for a specific range of IP addresses. Select Subnet to specify IP addresses on a network by their subnet mask.
IP Address Start	When the Local Address Type field is configured to Single , enter a (static) IP address on the LAN behind your ZyXEL Device. When the Local Address Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the Local Address Type field is configured to Subnet , this is a (static) IP address on the LAN behind your ZyXEL Device.
End / Subnet Mask	When the Local Address Type field is configured to Single , this field is N/A. When the Local Address Type field is configured to Range , enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the Local Address Type field is configured to Subnet , this is a subnet mask on the LAN behind your ZyXEL Device.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose Single , Range , or Subnet . Select Single with a single IP address. Select Range for a specific range of IP addresses. Select Subnet to specify IP addresses on a network by their subnet mask.
IP Address Start	When the Remote Address Type field is configured to Single , enter a (static) IP address on the network behind the remote IPSec router. When the Remote Address Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Remote Address Type field is configured to Subnet , enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the Remote Address Type field is configured to Single , this field is N/A. When the Remote Address Type field is configured to Range , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Remote Address Type field is configured to Subnet , enter a subnet mask on the network behind the remote IPSec router.
Address Information	

Table 95 VPN: Manual Key (continued)

LABEL	DESCRIPTION
My IP Address	Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as 0.0.0.0 : The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel. If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Security Protocol	
IPSec Protocol	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH . If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described next).
Encryption Algorithm	Select DES , 3DES or NULL from the drop-down list box. When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES . It also requires more processing power, resulting in increased latency and decreased throughput. Select NULL to set up a tunnel without encryption. When you select NULL , you do not enter an encryption key.
Encapsulation Key (only with ESP)	With DES , type a unique key 8 characters long. With 3DES , type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slower. Select MD5 for minimal security and SHA1 for maximum security.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for MD5 authentication or 20 characters for SHA1 authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

17.16 Viewing SA Monitor

Click **Security**, **VPN** and **Monitor** to open the **SA Monitor** screen as shown. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See [Section 17.6 on page 245](#) on keep alive to have the ZyXEL Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 137 VPN: SA Monitor

No.	Name	Encapsulation	IP Sec Algorithm
1	-	-	-
2	-	-	-
3	-	-	-
4	-	-	-
5	-	-	-
6	-	-	-
7	-	-	-
8	-	-	-
9	-	-	-
10	-	-	-
11	-	-	-
12	-	-	-
13	-	-	-
14	-	-	-
15	-	-	-
16	-	-	-
17	-	-	-
18	-	-	-
19	-	-	-
20	-	-	-

Disconnect **Refresh**

The following table describes the fields in this screen.

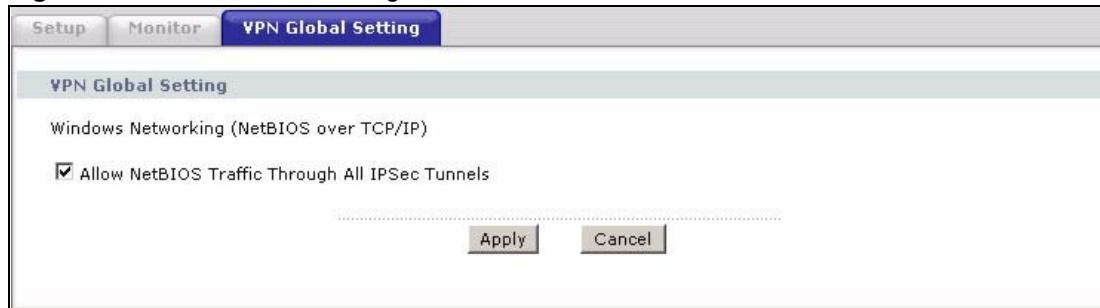
Table 96 VPN: SA Monitor

LABEL	DESCRIPTION
No	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays Tunnel or Transport mode.
IPSec Algorithm	This field displays the security protocol, encryption algorithm, and authentication algorithm used in each VPN tunnel.
Disconnect	Select one of the security associations, and then click Disconnect to stop that security association.
Refresh	Click Refresh to display the current active VPN connection(s).

17.17 Configuring Global Setting

To change your ZyXEL Device's global settings, click **VPN** and then **Global Setting**. The screen appears as shown.

Figure 138 VPN: Global Setting



The following table describes the fields in this screen.

Table 97 VPN: Global Setting

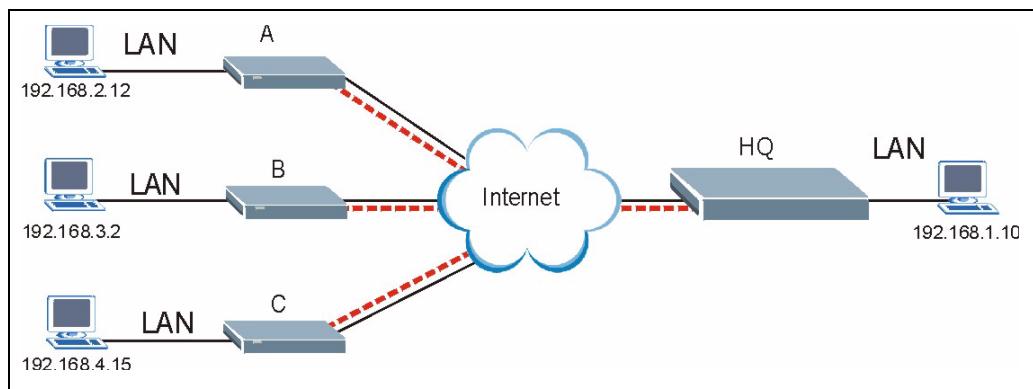
LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow NetBIOS Traffic Through All IPSec Tunnels	Select this check box to send NetBIOS packets through the VPN connection.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

17.18 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyXEL Device at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyXEL Device at headquarters has a static public IP address.

17.18.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (A, B and C in the figure) to use one VPN rule to simultaneously access a ZyXEL Device at headquarters (HQ in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 139 Telecommuters Sharing One VPN Rule Example**Table 98** Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (N/A)

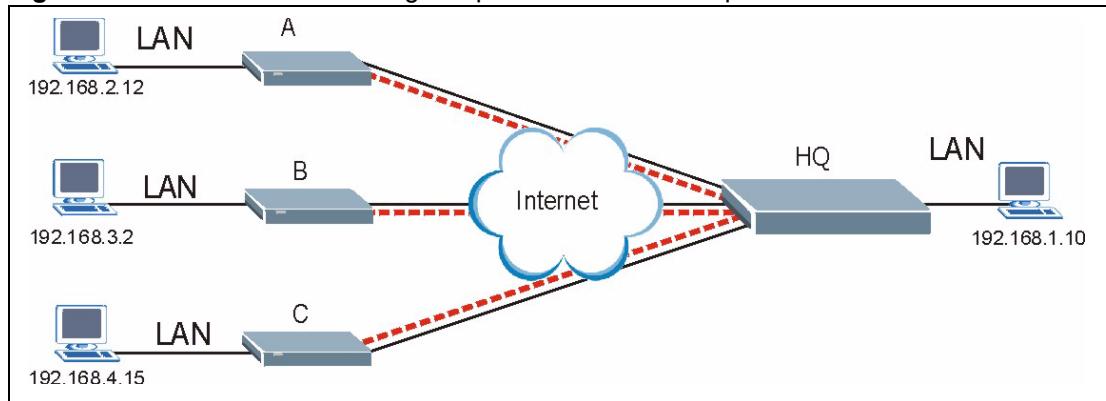
17.18.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see[Section 17.12.1 on page 255](#)), the ZyXEL Device can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyXEL Device at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyXEL Device at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyXEL Device located at headquarters. The ZyXEL Device at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyXEL Device at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

Figure 140 Telecommuters Using Unique VPN Rules Example**Table 99** Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My IP Address 0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters ZyXEL Device Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters ZyXEL Device Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters ZyXEL Device Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

17.19 VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote Management**) to allow access for that service.

CHAPTER 18

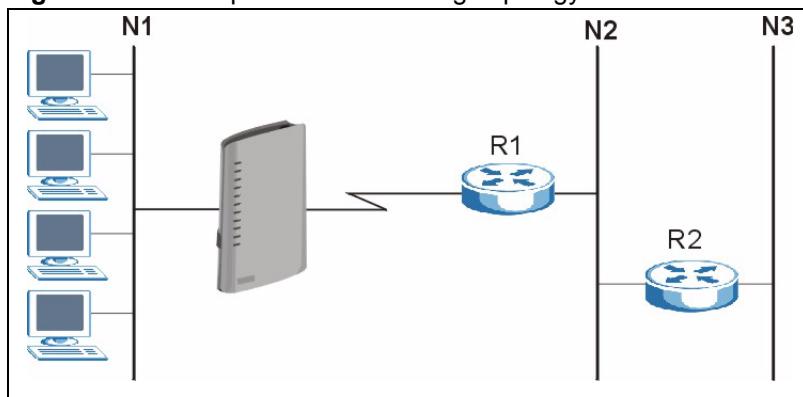
Static Route

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

18.1 Static Route

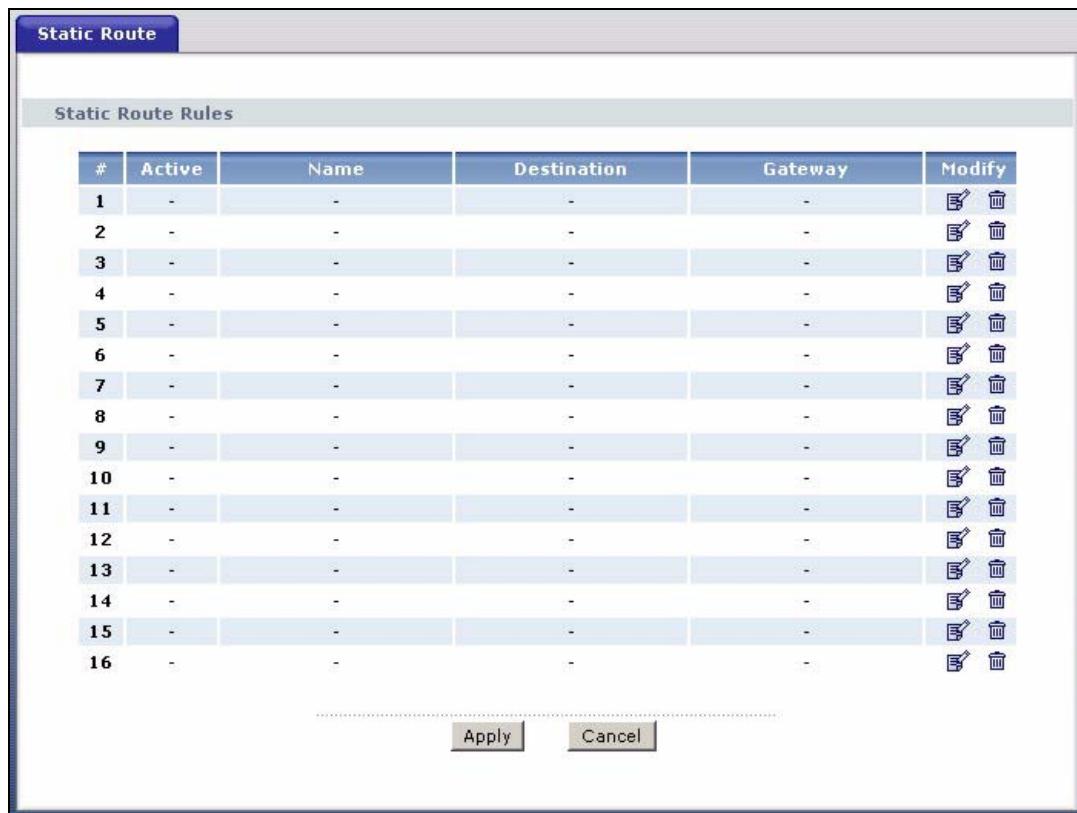
Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route 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 141 Example of Static Routing Topology



18.2 Configuring Static Route

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

Figure 142 Static Route

The following table describes the labels in this screen.

Table 100 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.

18.2.1 Static Route Edit

Click a static route's edit icon to open the following screen. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 143 Static Route Edit

The screenshot shows a configuration interface titled "Static Route Setup". It includes the following fields:

- Active:** A checkbox labeled "Active".
- Route Name:** An input field containing the value "0.0.0.0".
- Destination IP Address:** An input field containing the value "0.0.0.0".
- IP Subnet Mask:** An input field containing the value "0.0.0.0".
- Gateway IP Address:** An input field containing the value "0.0.0.0".

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

The following table describes the labels in this screen.

Table 101 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 to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 19

Bandwidth Management

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

19.1 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.

The sum of the bandwidth allotments that apply to any interface must be less than or equal to the speed allocated to that interface in the **Bandwidth Management Summary** screen.

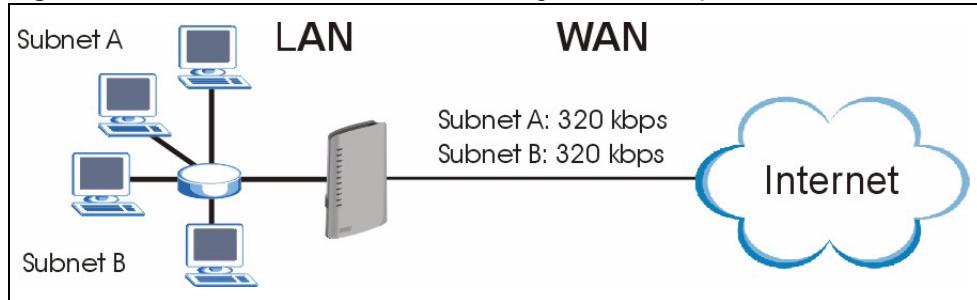
19.2 Application-based Bandwidth Management

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

19.3 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 144 Subnet-based Bandwidth Management Example

19.4 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 102 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

19.5 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.

19.5.1 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.

19.5.2 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.

19.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see [Figure 145 on page 278](#)) 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 unallocated 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.

19.6.1 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 unallocated. Make sure that the interface's root class has more bandwidth than the sum of the bandwidths of the interface's bandwidth management rules.

19.6.2 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 unallocated 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 103 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 unallocated 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 unallocated and unused bandwidth among the classes that require more bandwidth.

19.6.2.1 Priority-based Allotment of Unused and Unallocated Bandwidth

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

Table 104 Priority-based Allotment of Unused and Unallocated 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 unallocated 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 unallocated and unused bandwidth goes to the higher priority sales and marketing classes.

19.6.2.2 Fairness-based Allotment of Unused and Unallocated Bandwidth

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

Table 105 Fairness-based Allotment of Unused and Unallocated 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 unallocated 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.

19.6.3 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 106 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.

19.7 Over Allotment of Bandwidth

You can set the bandwidth management speed for an interface higher than the interface’s actual transmission speed. Higher priority traffic gets to use up to its allocated bandwidth, even if it takes up all of the interface’s available bandwidth. This could stop lower priority traffic from being sent. The following is an example.

Table 107 Over Allotment of Bandwidth Example

BANDWIDTH CLASSES, ALLOTMENTS	PRIORITIES
Actual outgoing bandwidth available on the interface: 1000 kbps	
Root Class: 1500 kbps (same as Speed setting)	High
VoIP traffic (Service = SIP): 500 Kbps	High
NetMeeting traffic (Service = H.323): 500 kbps	High
FTP (Service = FTP): 500 Kbps	Medium

If you use VoIP and NetMeeting at the same time, the device allocates up to 500 Kbps of bandwidth to each of them before it allocates any bandwidth to FTP. As a result, FTP can only use bandwidth when VoIP and NetMeeting do not use all of their allocated bandwidth.

Suppose you try to browse the web too. In this case, VoIP, NetMeeting and FTP all have higher priority, so they get to use the bandwidth first. You can only browse the web when VoIP, NetMeeting, and FTP do not use all 1000 Kbps of available bandwidth.

19.8 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 145 Bandwidth Management: Summary

Interface	Active	Speed(kbps)	Scheduler	Max Bandwidth Usage
LAN	<input checked="" type="checkbox"/>	100000	Priority-Based	<input checked="" type="checkbox"/> Yes
WLAN	<input checked="" type="checkbox"/>	54000	Priority-Based	<input checked="" type="checkbox"/> Yes
WAN	<input checked="" type="checkbox"/>	800	Priority-Based	<input checked="" type="checkbox"/> Yes

Buttons at the bottom: Apply, Cancel

The following table describes the labels in this screen.

Table 108 Media Bandwidth Management: Summary

LABEL	DESCRIPTION
Interface	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. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. 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. You can set this number higher than the interface's actual transmission speed. This will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. You can also set this number lower than the interface's actual transmission speed. If you do not enable Max Bandwidth Usage , this will cause the ZyXEL Device to not use some of the interface's available bandwidth.
Scheduler	Select either Priority-Based or Fairness-Based from the drop-down menu to control the traffic flow. Select Priority-Based to give preference to bandwidth classes with higher priorities. Select Fairness-Based to treat all bandwidth classes equally.

Table 108 Media Bandwidth Management: Summary (continued)

LABEL	DESCRIPTION
Max Bandwidth Usage	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).
Apply	Click Apply to save your settings to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

19.9 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 146 Bandwidth Management: Rule Setup

The screenshot shows the 'Rule Setup' tab selected in the top navigation bar. Below it, there are dropdown menus for 'Direction' (set to LAN), 'Service' (set to WWW), 'Priority' (set to High), and a bandwidth value of '10 (kbps)'. An 'Add' button is located to the right of the priority dropdown. The main area is titled 'To LAN Interface' and contains a table of rules:

#	Active	Rule Name	Destination Port	Priority	Bandwidth(kbps)	Modify
1	<input checked="" type="checkbox"/>	WWW	0	Low	10	
2	<input checked="" type="checkbox"/>	FTP	0	Mid	10	
3	<input checked="" type="checkbox"/>	E-Mail	0	Mid	10	
4	<input checked="" type="checkbox"/>	Telnet	0	Low	10	
5	<input checked="" type="checkbox"/>	NetMeeting (H.323)	0	Mid	10	
6	<input checked="" type="checkbox"/>	VoIP (SIP)	0	High	10	
7	<input checked="" type="checkbox"/>	VoIP (H.323)	0	High	10	
8	<input checked="" type="checkbox"/>	TFTP	0	Low	10	

At the bottom of the screen are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 109 Bandwidth Management: Rule Setup

LABEL	DESCRIPTION
Direction	Select the direction of traffic to which you want to apply bandwidth management.
Service	Select a service for your rule or you can select User define to go to the screen where you can define your own.

Table 109 Bandwidth Management: Rule Setup (continued)

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

19.9.1 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. See [Appendix G on page 407](#) for a list of commonly used services and port numbers.

Figure 147 Bandwidth Management Rule Configuration

The following table describes the labels in this screen.

Table 110 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.
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	

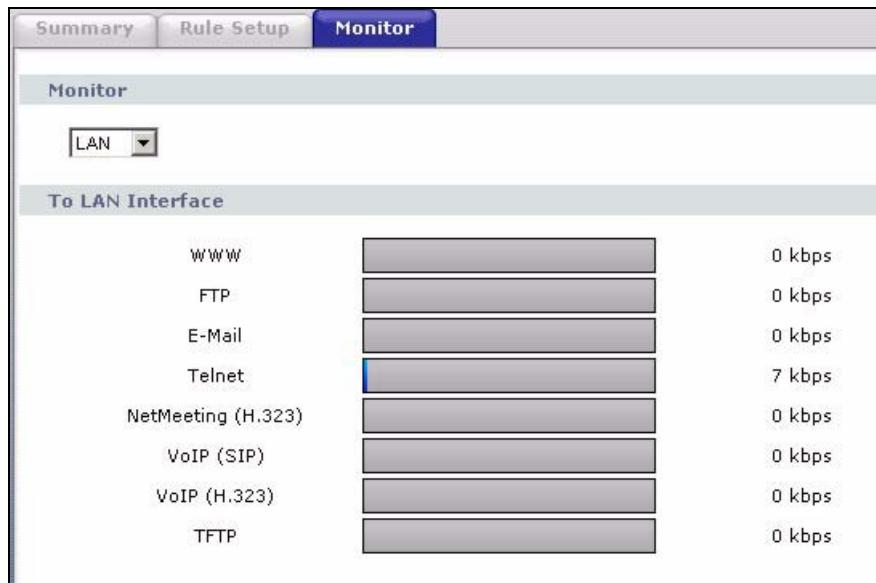
Table 110 Bandwidth Management Rule Configuration (continued)

LABEL	DESCRIPTION
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 appendices for more information on IP subnetting.
Destination Port	Enter the port number of the destination. 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 appendices for more information on IP subnetting. A blank source port means any source port number.
Source Port	Enter the port number of the source.
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.
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

19.10 Bandwidth Monitor

To view the ZyXEL Device's bandwidth usage, 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. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 148 Bandwidth Management: Monitor



CHAPTER 20

Dynamic DNS Setup

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

20.1 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 stays the same 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.

20.1.1 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.

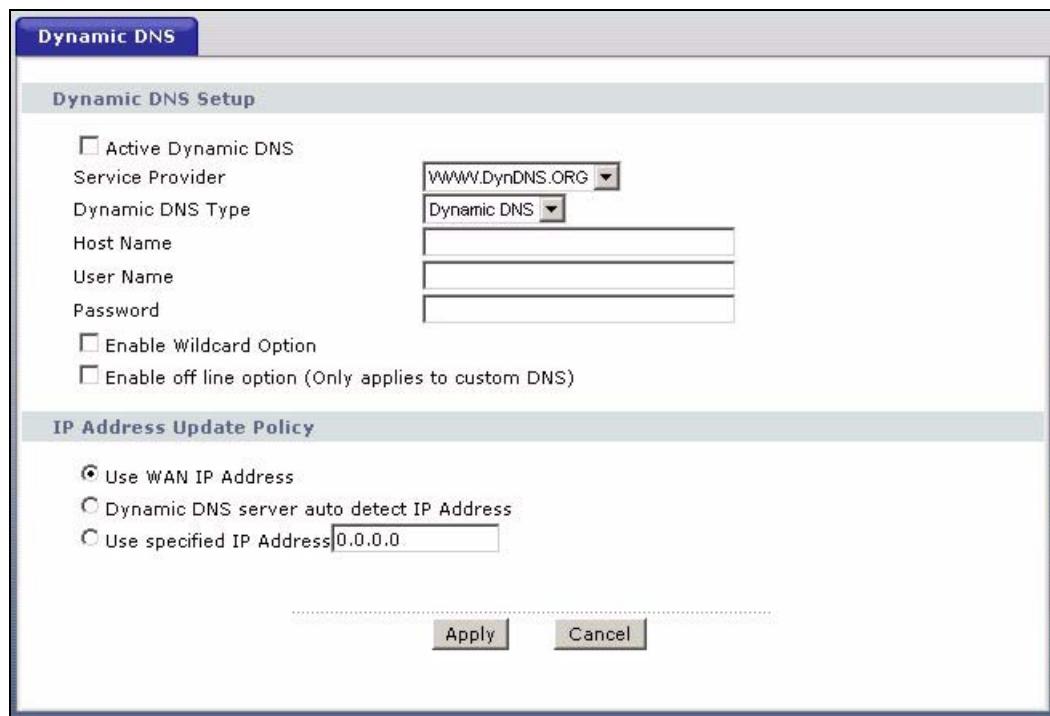
If you have a private WAN IP address, then you cannot use Dynamic DNS.

See [Section 20.2 on page 285](#) for configuration instruction.

20.2 Configuring Dynamic DNS

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

See [Section 20.1 on page 285](#) for more information.

Figure 149 Dynamic DNS

The following table describes the fields in this screen.

Table 111 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 111 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 to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 21

Remote Management Configuration

This chapter provides information on configuring remote management.

21.1 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 **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

21.1.1 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.

21.1.2 Remote Management and NAT

When NAT is enabled:

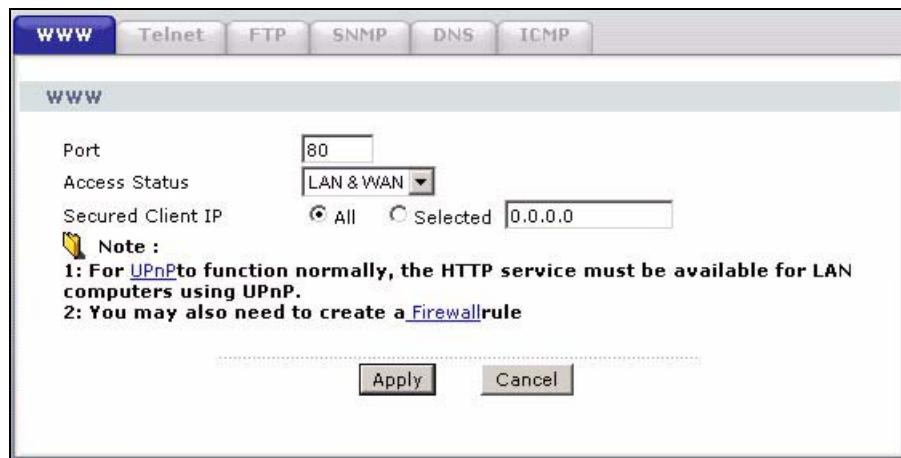
- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

21.1.3 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.

21.2 WWW

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

Figure 150 Remote Management: WWW

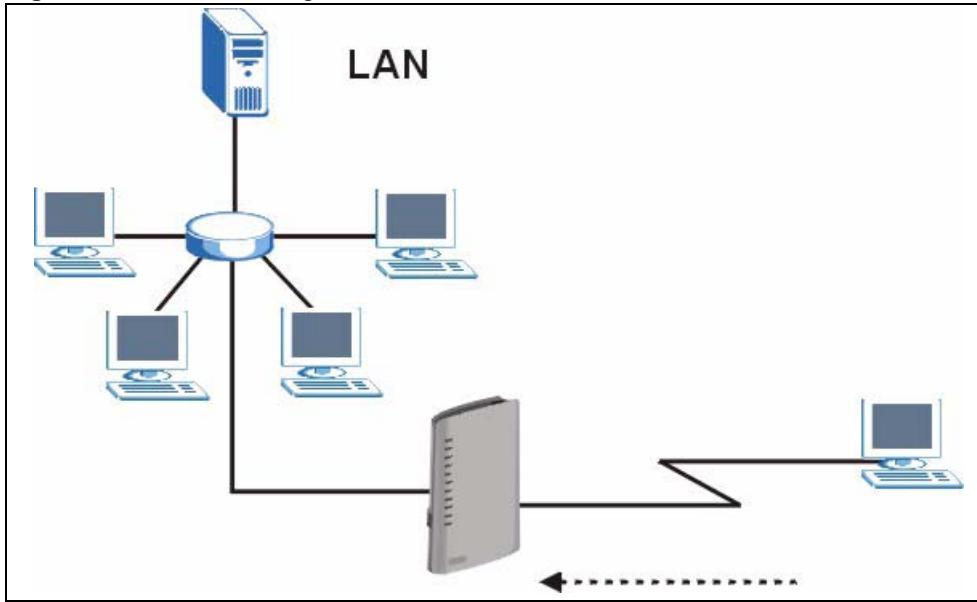
The following table describes the labels in this screen.

Table 112 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 to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

21.3 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 151 Telnet Configuration on a TCP/IP Network

21.4 Configuring Telnet

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

Figure 152 Remote Management: Telnet

Port	23
Access Status	LAN & WAN
Secured Client IP	<input checked="" type="radio"/> All <input type="radio"/> Selected 0.0.0.0
Note : You may also need to create a Firewallrule	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 113 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.

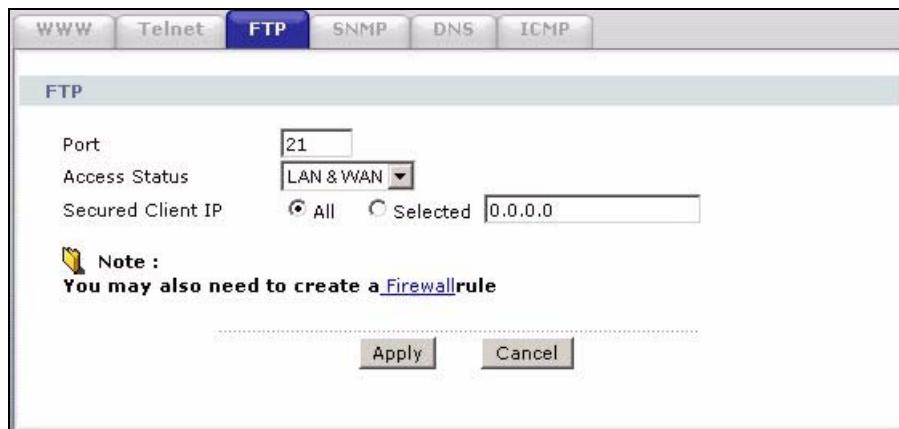
Table 113 Remote Management: Telnet

LABEL	DESCRIPTION
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.

21.5 Configuring FTP

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

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

Figure 153 Remote Management: FTP

The following table describes the labels in this screen.

Table 114 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.

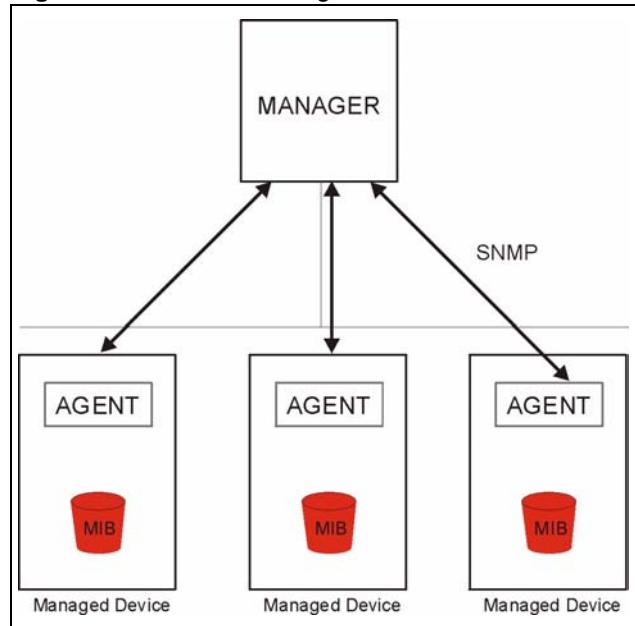
Table 114 Remote Management: FTP

LABEL	DESCRIPTION
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.

21.6 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 154 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.

21.6.1 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.

21.6.2 SNMP Traps

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

Table 115 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).

Table 115 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
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, CI 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.

21.6.3 Configuring SNMP

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

Figure 155 Remote Management: SNMP

The screenshot shows the 'SNMP' configuration page. At the top, there are tabs for WWW, Telnet, FTP, SNMP (which is selected and highlighted in blue), DNS, and ICMP. The main area is titled 'SNMP'. It contains the following fields:

- Port:** 161
- Access Status:** LAN & WAN
- Secured Client IP:** Radio button for 'All' is selected, and the input field shows 0.0.0.0.

Below this is a section titled 'SNMP Configuration' with the following fields:

- Get Community:** public
- Set Community:** public
- TrapCommunity:** public
- TrapDestination:** 0.0.0.0

At the bottom of the screen, there is a note: **Note :** You may also need to create a [Firewall rule](#).

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

The following table describes the labels in this screen.

Table 116 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.

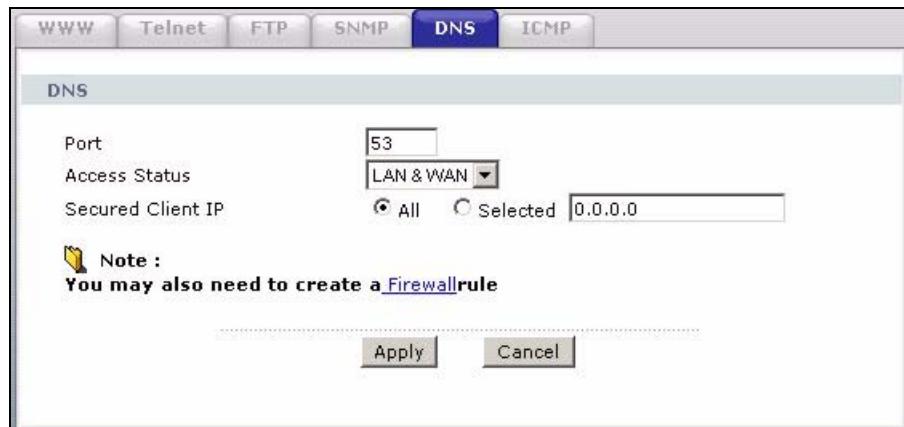
Table 116 Remote Management: SNMP

LABEL	DESCRIPTION
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.

21.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on LAN 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 156 Remote Management: DNS

The following table describes the labels in this screen.

Table 117 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.

21.8 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.

Figure 157 Remote Management: ICMP

The following table describes the labels in this screen.

Table 118 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 corresponding firewall policy to send a TCP reset packet for a blocked TCP packet or an ICMP port-unreachable packet for a blocked UDP packets or just drop the packets 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 22

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

22.1 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 22.2.1 on page 302](#) for configuration instructions.

22.1.1 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.

22.1.2 NAT Traversal

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

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

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

See the NAT chapter for more information on NAT.

22.1.3 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.

22.2 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.

22.2.1 Configuring UPnP

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

See [Section 22.1 on page 301](#) for more information.

Figure 158 Configuring UPnP

The following table describes the fields in this screen.

Table 119 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.

22.3 Installing UPnP in Windows Example

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

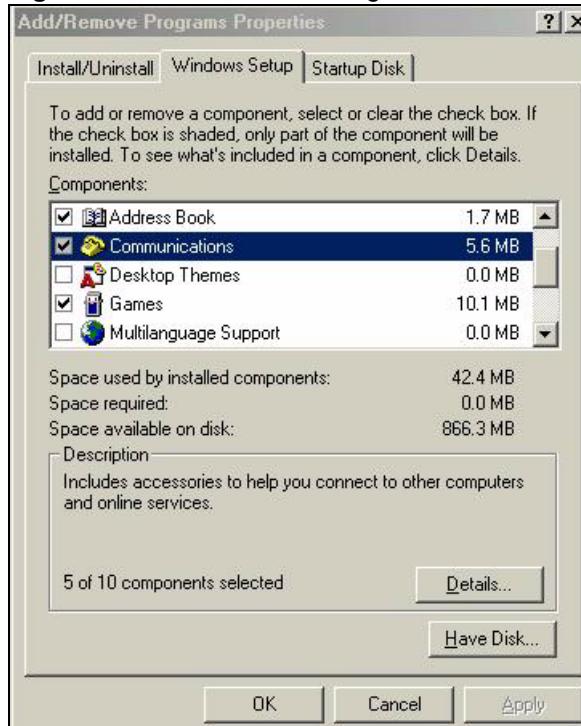
Installing UPnP in Windows Me

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

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

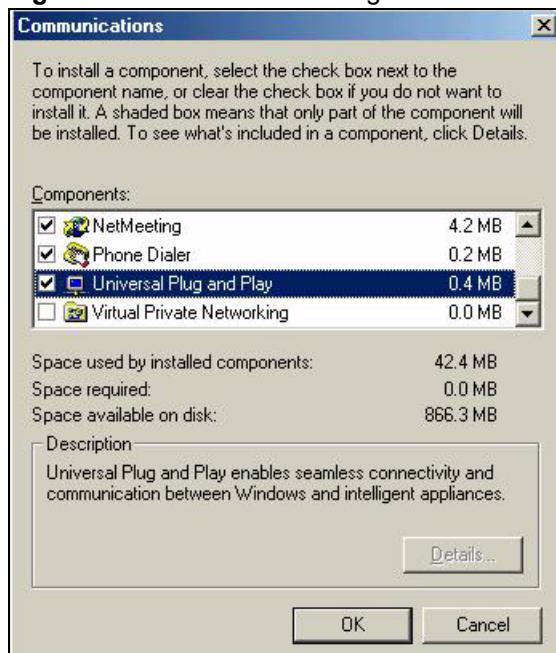
- 2** Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 159 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 160 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

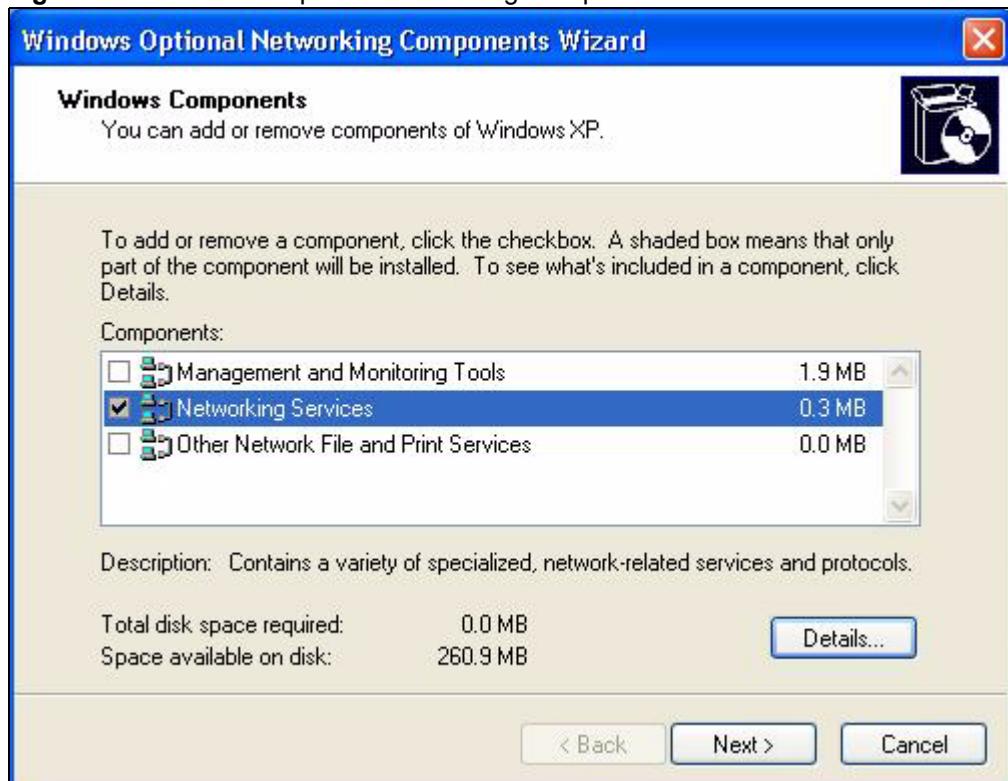
Follow the steps below to install the UPnP in Windows XP.

- 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**

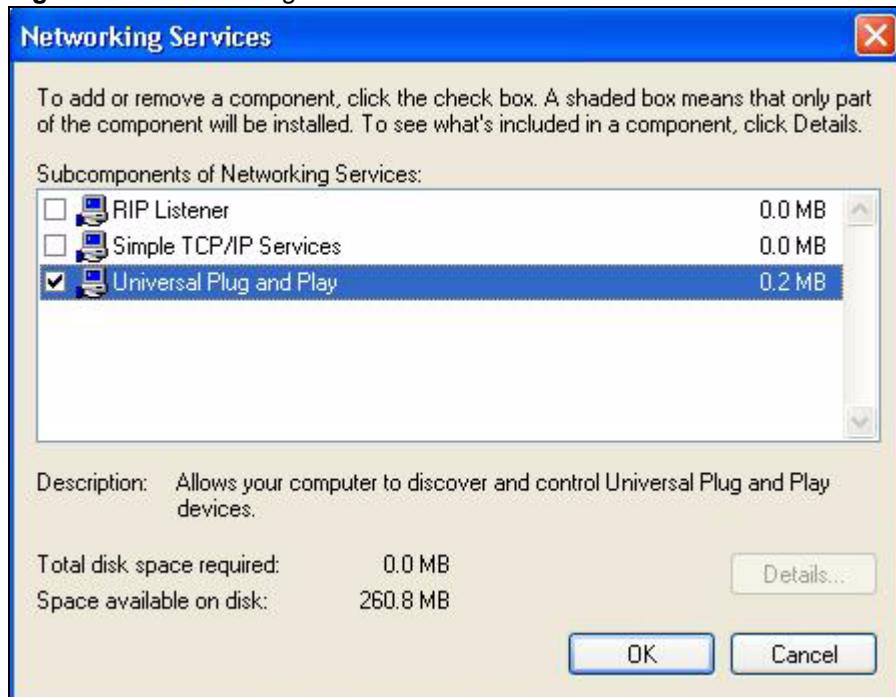
Figure 161 Network Connections



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

Figure 162 Windows Optional Networking Components Wizard

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

Figure 163 Networking Services

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

22.4 Using UPnP in Windows XP Example

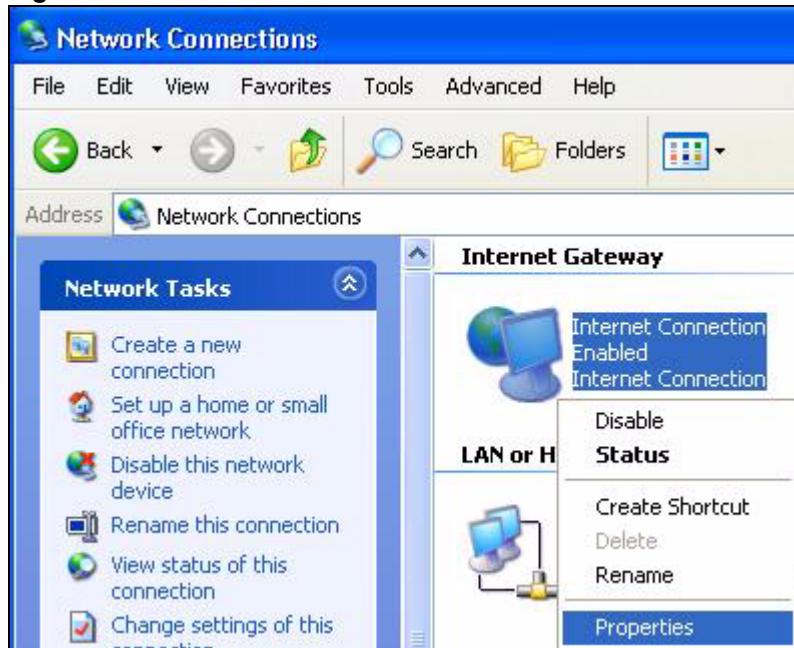
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

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 164 Network Connections

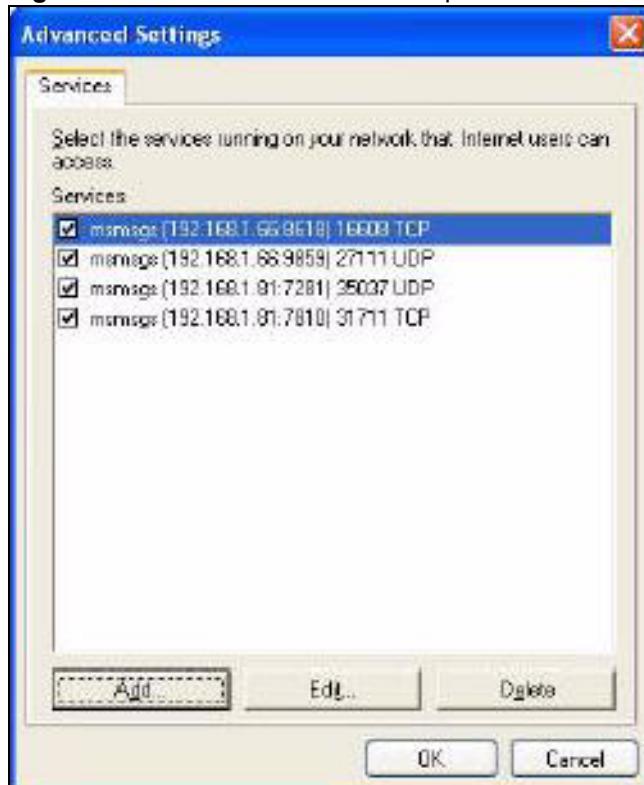
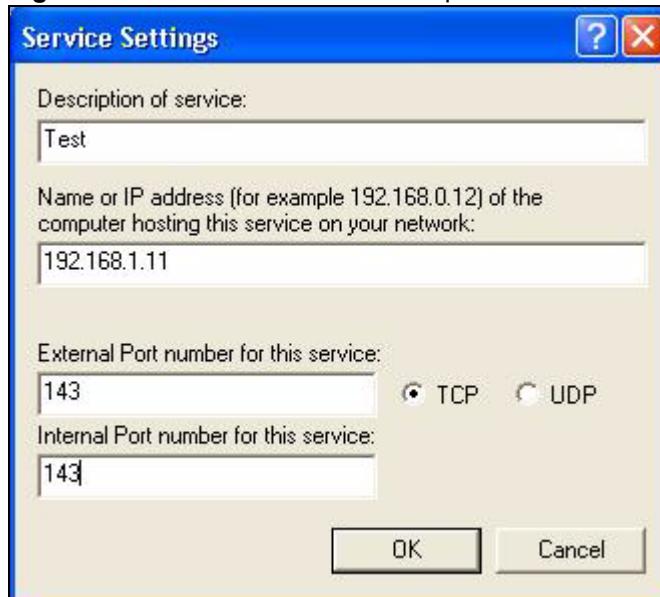


- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

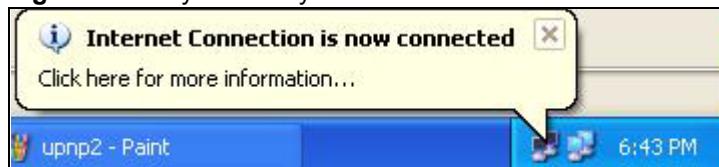
Figure 165 Internet Connection Properties



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

Figure 166 Internet Connection Properties: Advanced Settings**Figure 167** 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 168 System Tray Icon

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

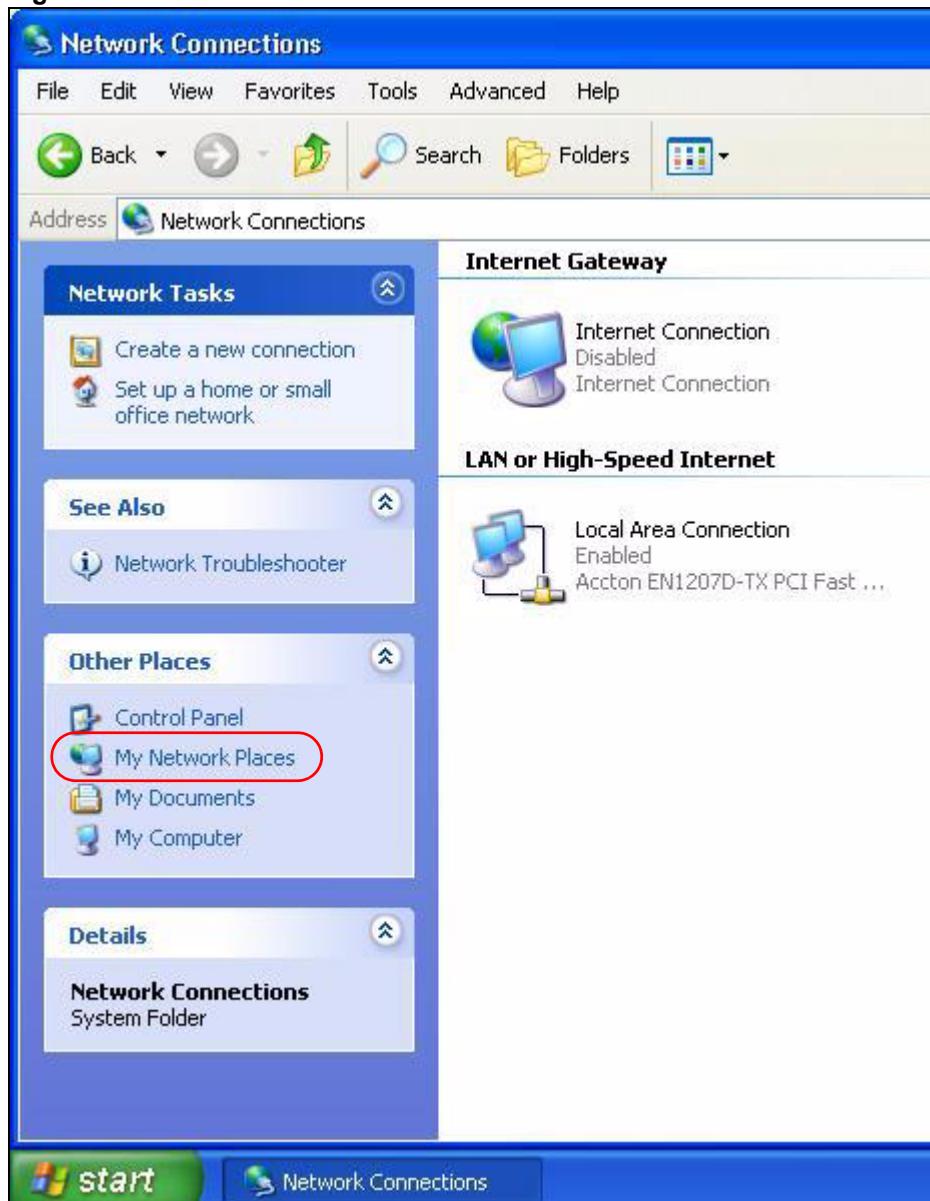
Figure 169 Internet Connection Status

Web Configurator Easy Access

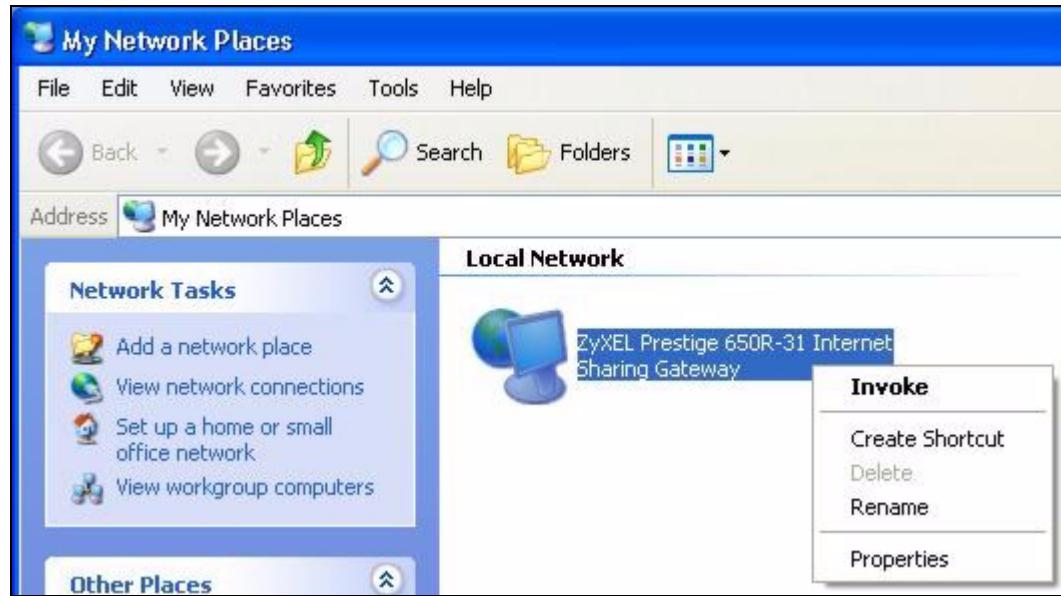
With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

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 170 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 171 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 172 Network Connections: My Network Places: Properties: Example

CHAPTER 23

System

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

23.1 General Setup and System Name

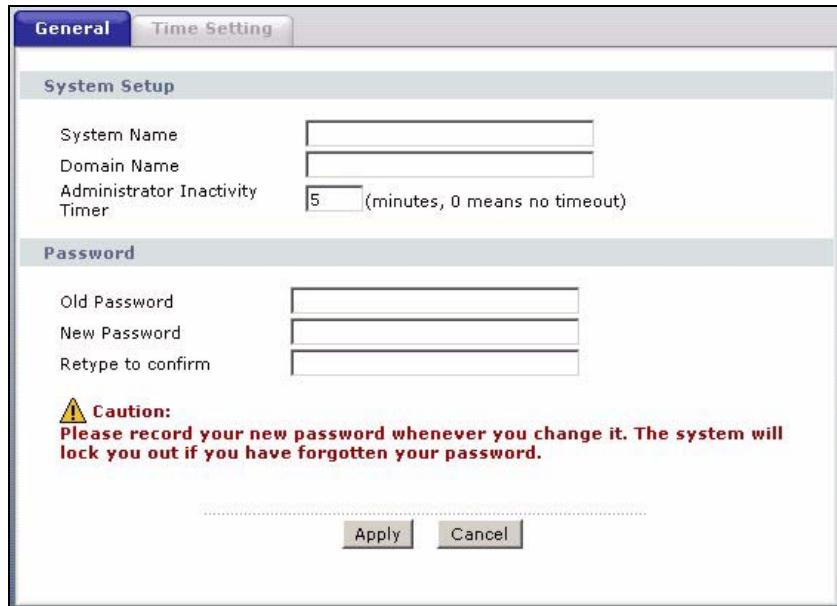
General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- 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**.

23.1.1 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 173 System General Setup

The following table describes the labels in this screen.

Table 120 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 to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

23.2 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 174 System Time Setting

The following table describes the fields in this screen.

Table 121 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 121 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). Select None to enter the time and date manually.
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).
Enable 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 121 System Time Setting (continued)

LABEL	DESCRIPTION
End Date	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: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Last, Sunday, October and type 2 in the o'clock field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 24

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.

24.1 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.

24.1.1 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.

24.2 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 24.3 on page 320](#)).

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 175 View Log

View Logs					
Display:		Email Log Now		Refresh	Clear 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 122 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.
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.
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.

24.3 Configuring Log Settings

Click **Maintenance > Logs > Log Settings** to open the following screen. Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device is to record. See [Section 24.1 on page 319](#) for more information.

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 176 Log Settings

E-mail Log Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject:

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Enable SMTP Authentication
User Name:
Password:

Log Schedule:

Day for Sending Log:

Time for Sending Log:

Clear log after sending mail

Syslog Logging

Active
Syslog IP Address: (Server Name or IP Address)
Log Facility:

Active Log and Alert

Log	Send Immediate Alert
<input type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors
<input type="checkbox"/> System Errors	<input type="checkbox"/> Access Control
<input type="checkbox"/> Access Control	<input type="checkbox"/> Blocked Web Sites
<input type="checkbox"/> UPnP	<input type="checkbox"/> Attacks
<input type="checkbox"/> Forward Web Sites	
<input type="checkbox"/> Blocked Web Sites	
<input type="checkbox"/> Attacks	
<input type="checkbox"/> Any IP	
<input type="checkbox"/> 802.1x	
<input type="checkbox"/> SIP	
<input type="checkbox"/> RTP	
<input type="checkbox"/> FSM	

The following table describes the fields in this screen.

Table 123 Log Settings

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

Table 123 Log Settings

LABEL	DESCRIPTION
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	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: Daily Weekly Hourly When Log is Full None . If you select Weekly or Daily , specify a time of day when the E-mail should be sent. If you select Weekly , then also specify which day of the week the E-mail should be sent. If you select When Log is Full , an alert is sent when the log fills up. If you select None , no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click Active to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
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.

24.4 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 124 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

24.4.1 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 177 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

24.5 Log Descriptions

This section provides descriptions of example log messages.

Table 125 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 (%s) 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 (%s) 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.

Table 125 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
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.

Table 126 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 127 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 (%d)) and was blocked or forwarded according to the rule.

Table 127 Access Control Logs (continued)

LOG MESSAGE	DESCRIPTION
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 128 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 timeout, 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 CI command: "sys firewall tcprst").

Table 129 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 (%d) and rule number (%d)) and was blocked or forwarded according to the rule.

For type and code details, see [Table 138 on page 330](#).

Table 130 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.
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 131 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 132 PPP Logs

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

Table 132 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 133 UPnP Logs

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

Table 134 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 138 on page 330](#).

Table 135 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.

Table 135 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
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.
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 136 802.1X Logs

LOG MESSAGE	DESCRIPTION
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.
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.
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.

Table 137 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 138 ICMP Notes

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

Table 138 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 139 Syslog Logs

LOG MESSAGE	DESCRIPTION
<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>	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.

Table 140 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 141 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 142 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 143 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.

CHAPTER 25

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.

25.1 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.

25.2 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 144 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

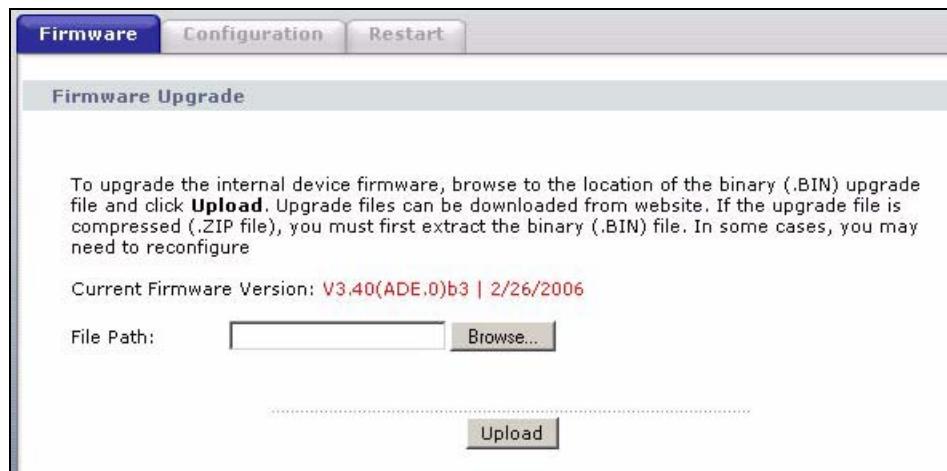
25.3 File Maintenance Over WAN

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.

25.4 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 25.9 on page 343](#) for upgrading firmware using FTP/TFTP commands.

Figure 178 Firmware Upgrade

The following table describes the labels in this screen.

Table 145 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 179 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 180 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 181 Firmware Upload Error Message

25.5 Backup and Restore

See [Section 25.8 on page 343](#) for information on 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 182 Configuration



25.5.1 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.

25.5.2 Restore Configuration

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

Table 146 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. Note: Attempting to upload files other than .rom configuration files could cause the ZyXEL Device to malfunction. If this happens, you will need to reset your ZyXEL Device, and will lose all your saved settings.
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 183 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 184 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 B on page 369](#) for details on how to set up your computer's IP address.

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

Figure 185 Configuration Upload Error

25.5.3 Reset to Factory Defaults

Clicking the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 186 Reset Warning 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 55](#) for more information on the **RESET** button.

25.6 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 187 Restart Screen



25.7 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.

25.7.1 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.

25.7.2 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 188 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

```

25.7.3 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 147 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).

25.7.4 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.

25.7.5 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.

25.7.6 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 148 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 25.3 on page 334](#) to read about configurations that disallow TFTP and FTP over WAN.

25.8 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.

25.8.1 Restore Using FTP Session Example

Figure 189 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 25.3 on page 334](#) to read about configurations that disallow TFTP and FTP over WAN.

25.9 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.

25.9.1 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.

25.9.2 FTP Session Example of Firmware File Upload

Figure 190 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 25.3 on page 334](#) to read about configurations that disallow TFTP and FTP over WAN.

25.9.3 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.

25.9.4 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 26

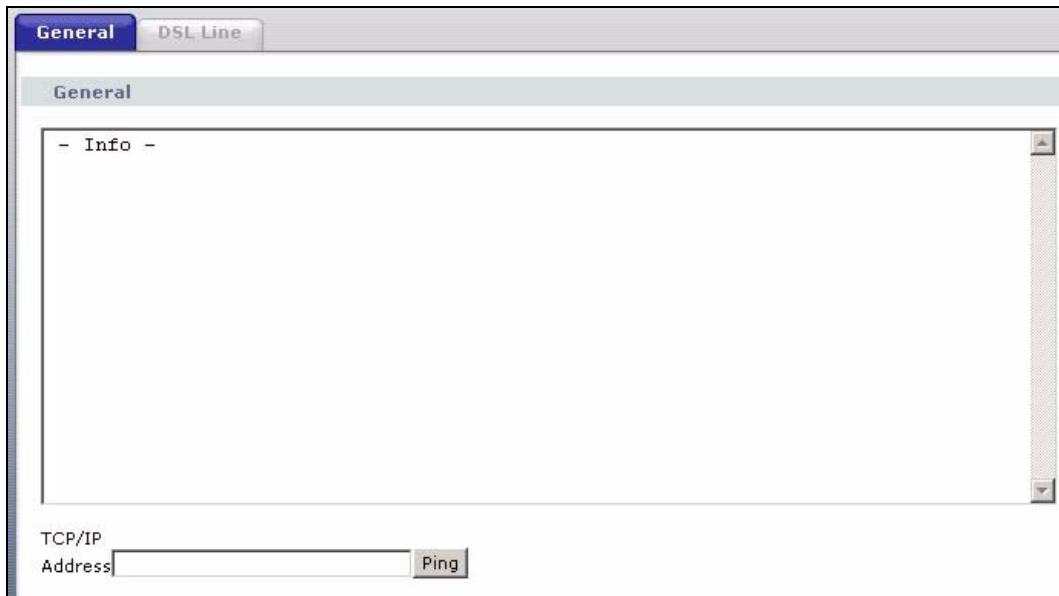
Diagnostic

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

26.1 General Diagnostic

Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 191 Diagnostic: General



The following table describes the fields in this screen.

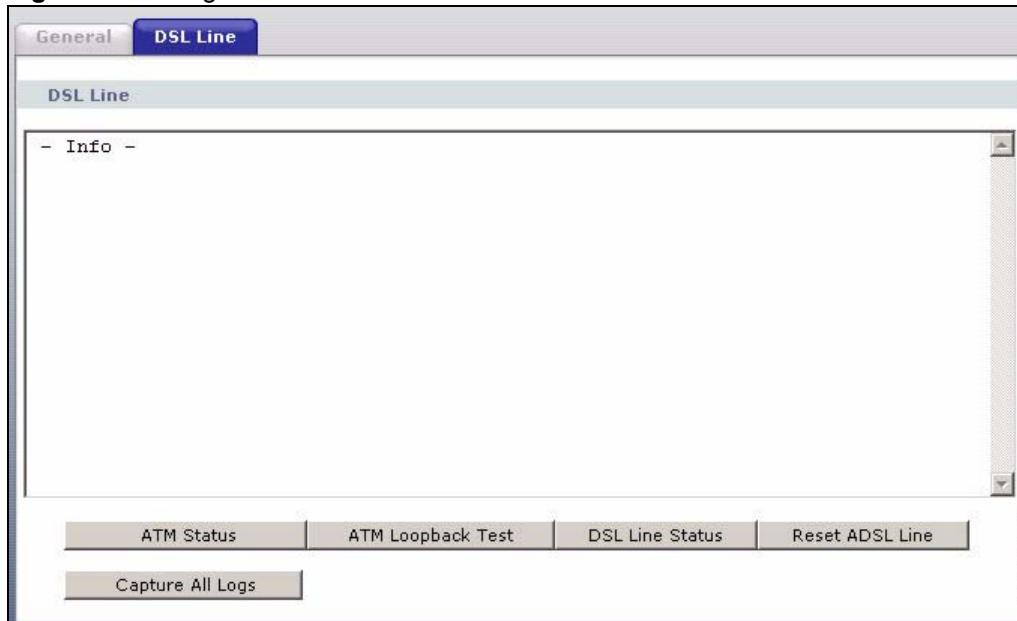
Table 149 Diagnostic: General

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.

26.2 DSL Line Diagnostic

Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

Figure 192 Diagnostic: DSL Line



The following table describes the fields in this screen.

Table 150 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 (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets.</p> <p>These counters are set back to zero whenever the device starts up.</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	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.
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>

Table 150 Diagnostic: DSL Line (continued)

LABEL	DESCRIPTION
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
Capture All Logs	Click this button to display information and statistics about your ZyXEL Device's ATM statistics, DSL connection statistics, DHCP settings, firmware version, WAN and gateway IP address, VPI/VCI and LAN IP address.

CHAPTER 27

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

27.1 Problems Starting Up the ZyXEL Device

Table 151 Troubleshooting Starting Up Your Device

PROBLEM	CORRECTIVE ACTION
None of the lights turn on when I turn on the ZyXEL Device.	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. Turn the ZyXEL Device off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

27.2 Problems with the LAN

Table 152 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN lights do not turn on.	Check your Ethernet cable connections (refer to the Quick Start Guide 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.

27.3 Problems with the WAN

Table 153 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 22.6.2 on page 286 .
I cannot get a WAN IP address from the ISP.	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 Chapter 6 on page 87 .
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 6 on page 87 . Make sure you entered the correct user name and password.
The Internet connection disconnects.	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to Section 6.2 on page 89 . Contact your ISP.

27.4 Problems Accessing the ZyXEL Device

Table 154 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 use the RESET button to restore all of the factory defaults including the password.</p>
I cannot access the web configurator.	<p>If you are using Internet Explorer in Windows XP or Windows Server 2003, make sure you allow pop-up windows, JavaScripts and Java permissions or set the Internet security level lower than High in Internet Explorer (in Internet Explorer, click Tools > Internet Options > Security > Custom Level...). See Section 27.4.1 on page 353 for more information.</p> <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 the chapter on remote management 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 Section 27.4.1 on page 353 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>

27.4.1 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.

27.4.1.1 Internet Explorer Pop-up Blockers

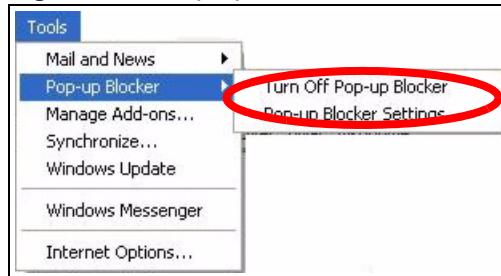
You may have to disable pop-up blocking to log into your device.

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.

27.4.1.1.1 Disable pop-up Blockers

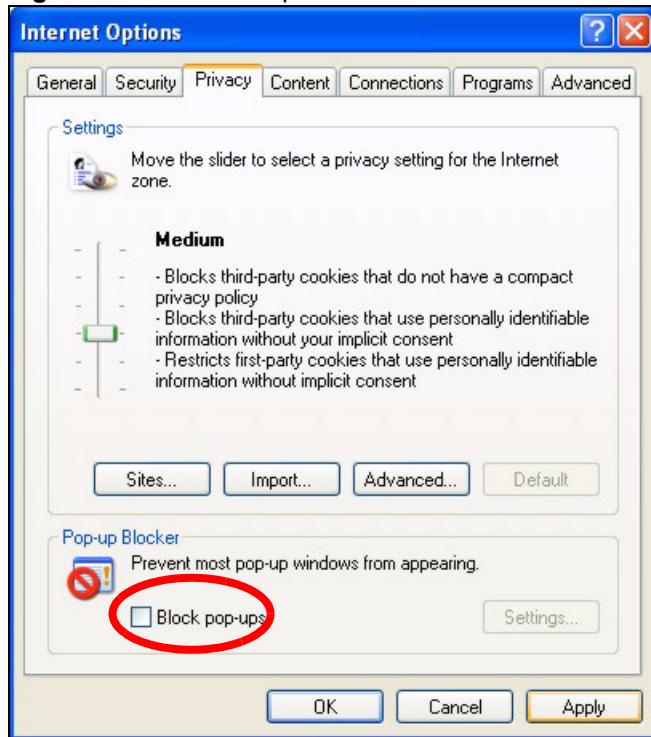
- 1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 193 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.

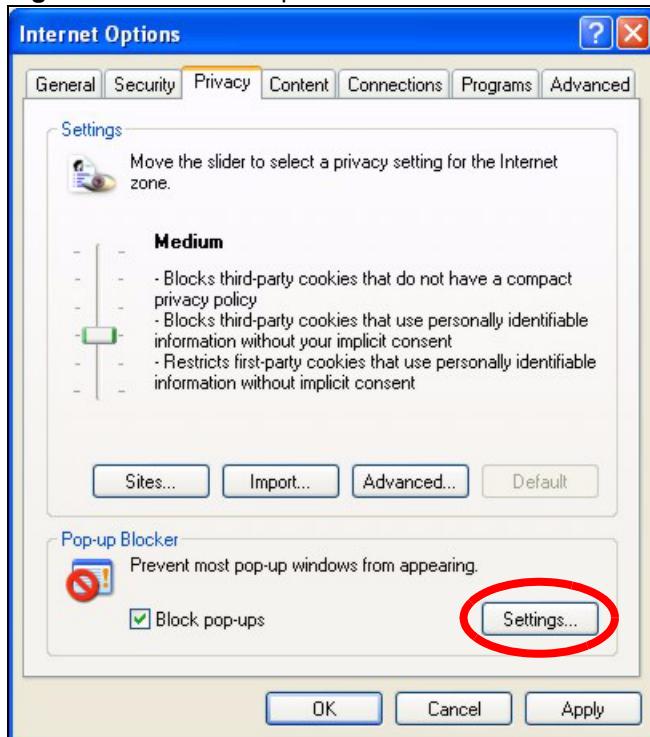
Figure 194 Internet Options

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

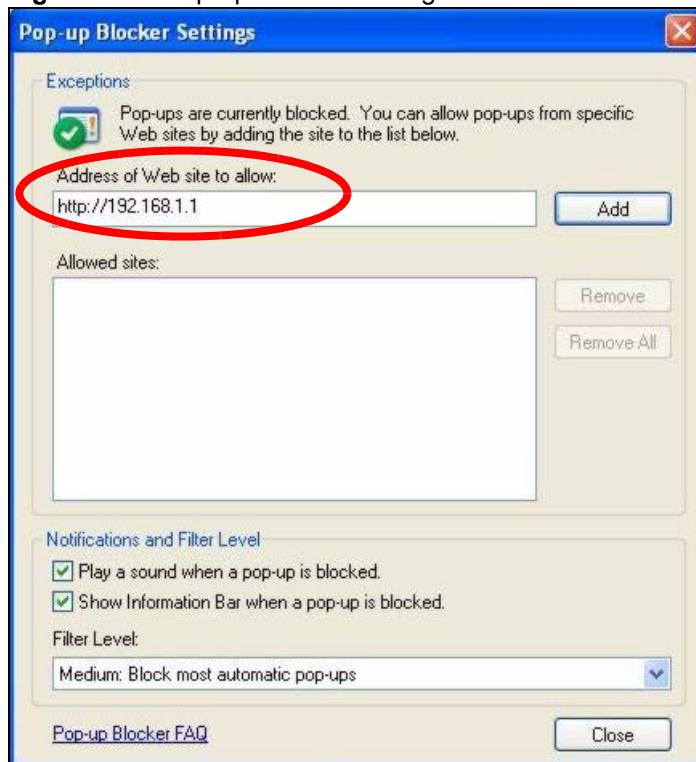
27.4.1.1.2 *Enable pop-up Blockers with Exceptions*

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 195 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 196 Pop-up Blocker Settings

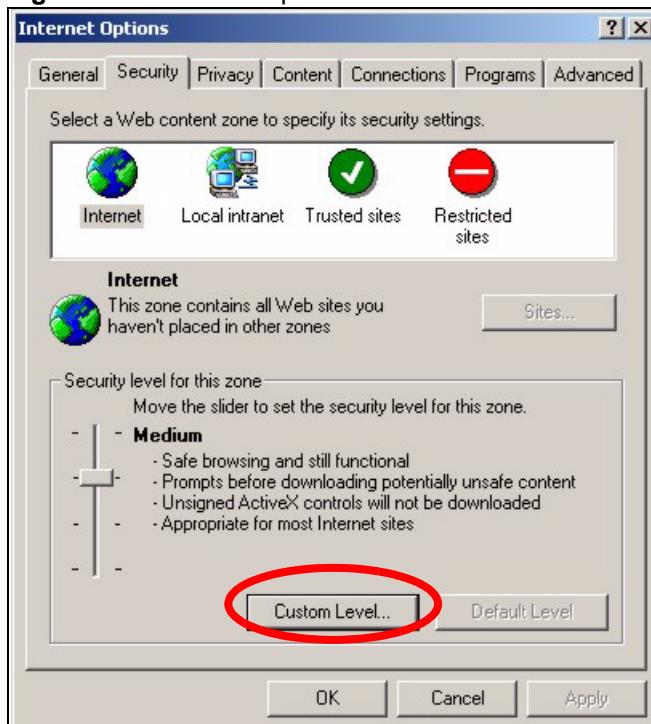
5 Click **Close** to return to the **Privacy** screen.

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

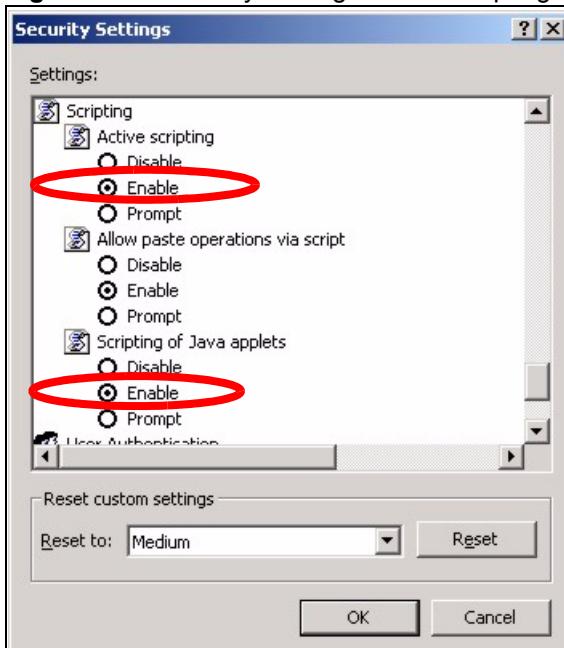
27.4.1.2 JavaScripts

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.

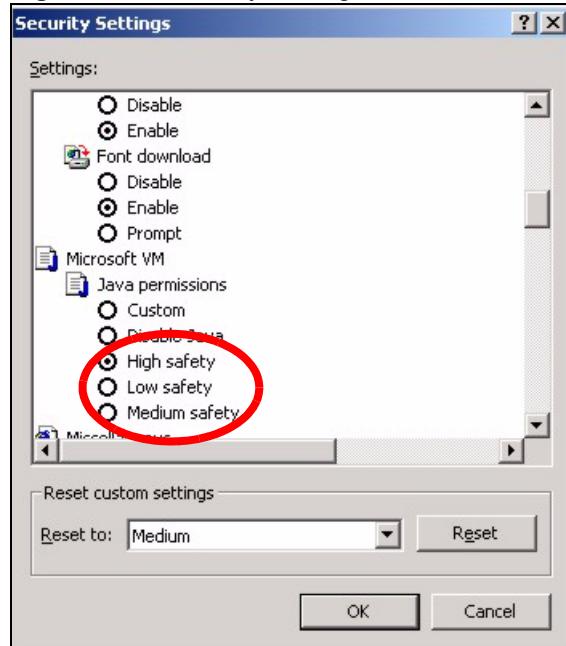
Figure 197 Internet Options

- 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 198 Security Settings - Java Scripting

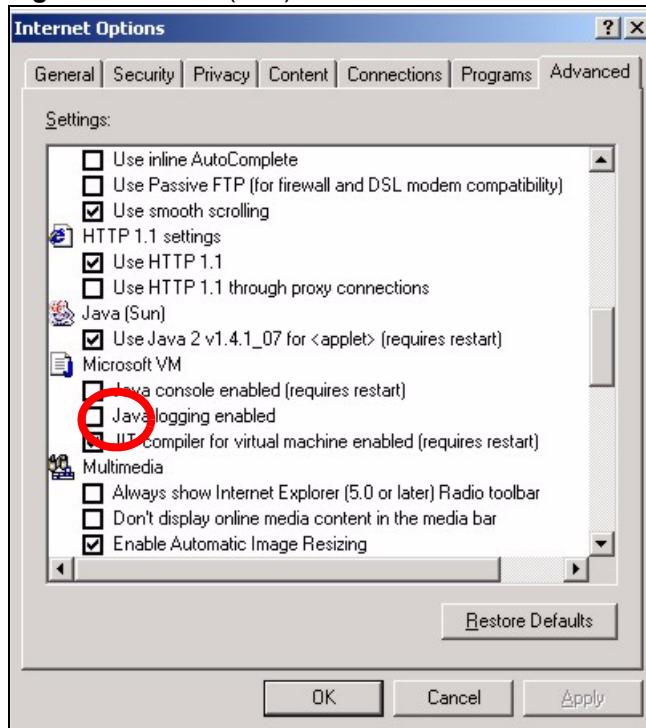
27.4.1.3 Java Permissions

- 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 199 Security Settings - Java

27.4.1.3.1 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 200 Java (Sun)

27.5 Telephone Problems

Table 155 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 or ISDN 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.

APPENDIX A

Product Specifications

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

Specification Tables

Table 156 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	192.168.1.32 to 192.168.1.64
Static DHCP Addresses	10
Dimensions	In mm: 165 (L) x 65 (D) x 242 (H)
Weight	600 g
Power Specification	18VDC 1A
DSL Port	1 RJ-45 port for AnnexB or UR-2
Ethernet Ports	4 auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
PHONE Ports	2 RJ-11 FXS POTS ports
ISDN PHONE Port	1 RJ-45 FXS ISDN port
PSTN/ISDN Port	1 RJ-45 FXO PSTN or ISDN port
RESET Button	Turns the wireless LAN radio on and off and restores factory defaults
Antenna	One attached external dipole antenna, 3dBi
Operation Temperature	0° C ~ 40° C
Storage Temperature	-20° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 95% RH

Table 157 Firmware Specifications

ADSL Standards	Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G-lite(G992.2)) EOC specified in ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL2 G-lite.bis (G.992.4) ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC 2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) RFC 1483 encapsulation over ATM VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols DHCP Server/Client/Relay RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy UPnP
Management	Embedded Web Configurator CLI (Command Line Interpreter) Remote Management via Telnet or Web SNMP manageable FTP/TFTP for firmware downloading, configuration backup and restoration Syslog Built-in Diagnostic Tools for FLASH memory, ADSL circuitry, RAM and LAN port
Wireless	IEEE 802.11g Compliance Frequency Range: 2.4 GHz Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: 54Mbps and Auto Fallback Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit. WLAN bridge to LAN Up to 32 MAC Address filters WPA, IEEE 802.1x External RADIUS server using EAP-MD5, TLS, TTLS

Table 157 Firmware Specifications (continued)

Firewall	Stateful Packet Inspection Prevents Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc. Real time E-mail alerts Reports and logs SIP ALG passthrough
NAT/SUA	Port Forwarding 512 NAT sessions Multimedia application PPTP under NAT/SUA IPSec passthrough SIP ALG passthrough
VPN	20 IPSec tunnels (2 concurrent) IKE and Manual Key Management AH and ESP Protocol DES, 3DES and AES Encryption SHA-1 and MD5 Authentication Tunnel and Transport Mode Encapsulation IPSec NAT Traversal NETBIOS pass-through for IPSec
Content Filtering	Web page blocking by URL keyword.
Static Routes	16 IP

Table 157 Firmware Specifications (continued)

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, G.729 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
Other Features	Any IP Zero Configuration (VC auto-hunting) Traffic Redirect Dynamic DNS IP Alias IP Policy Routing SPTGEN H.323 passthrough QoS

Power Adapter Specifications

Table 158 Power Adapter Specifications

NORTH AMERICAN PLUG STANDARDS	OEM (Original Equipment Manufacturer)	LEI (LEADER ELECTRONICS INC.)
AC Power Adapter Model	ADS18B-W 180100	MU18-2180100-A1
Input Power	AC 100~240Volts/50/60Hz/1A	AC 100~240Volts/50/60Hz/0.5A
Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	UL,CUL(UL 60950-1)	UL,CUL(UL 60950-1)
EUROPEAN PLUG STANDARDS		
AC Power Adapter Model	ADS18B-B 180100	MU18-2180100-C5
Input Power	AC 100~240Volts/50/60Hz/1A	AC 100~240Volts/50/60Hz/0.5A

Table 158 Power Adapter Specifications (continued)

Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	TUV, CE(EN 60950 -1)	TUV, CE(EN 60950-1)
UNITED KINGDOM PLUG STANDARDS		
AC Power Adapter Model	ADS18B-D 180100	MU18-2180100-B2
Input Power	AC 100~240Volts/50/60Hz/1A	AC 100~240Volts/50/60Hz/0.5A
Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	TUV, CE(EN 60950 -1)	TUV, CE(EN 60950-1)

APPENDIX B

Setting up Your Computer's IP Address

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

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

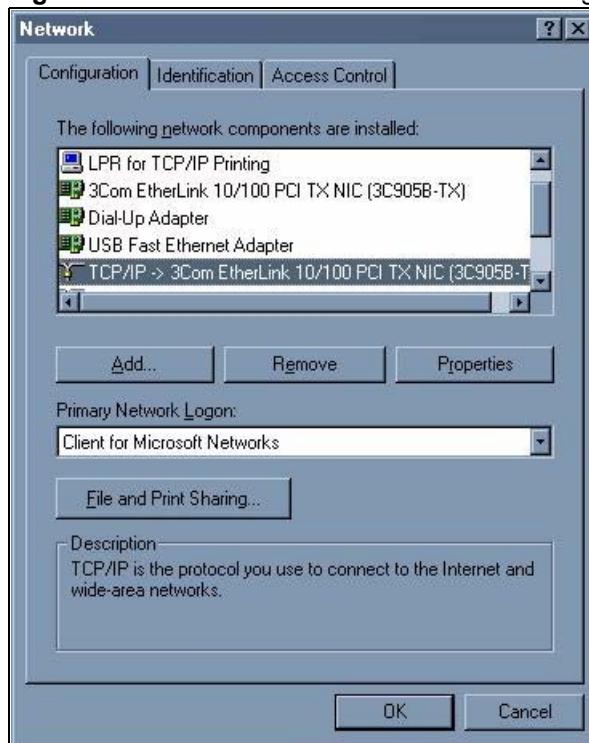
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

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

Windows 95/98/Me

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

Figure 201 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:

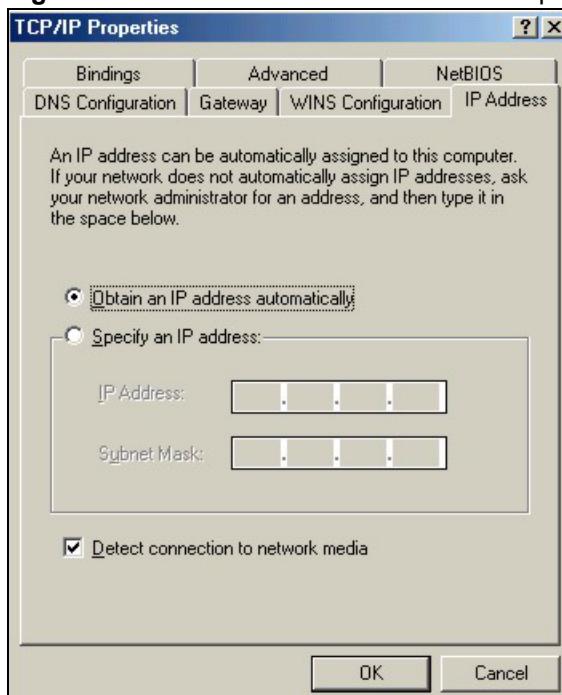
- 1** Click **Add**.
- 2** Select **Client** and then click **Add**.

- 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.

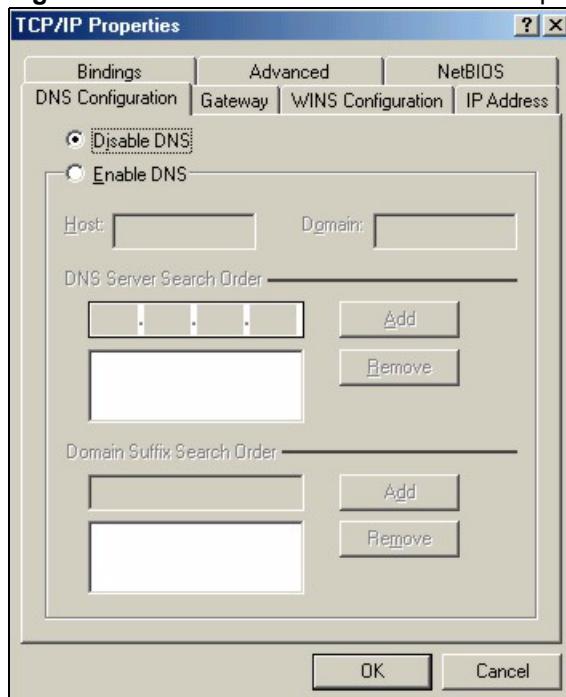
Configuring

- 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 202 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 203 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

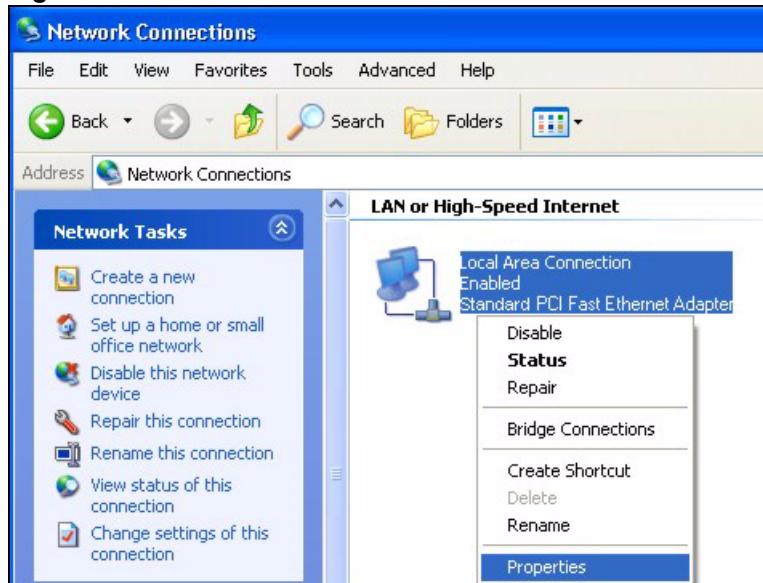
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 204 Windows XP: Start Menu

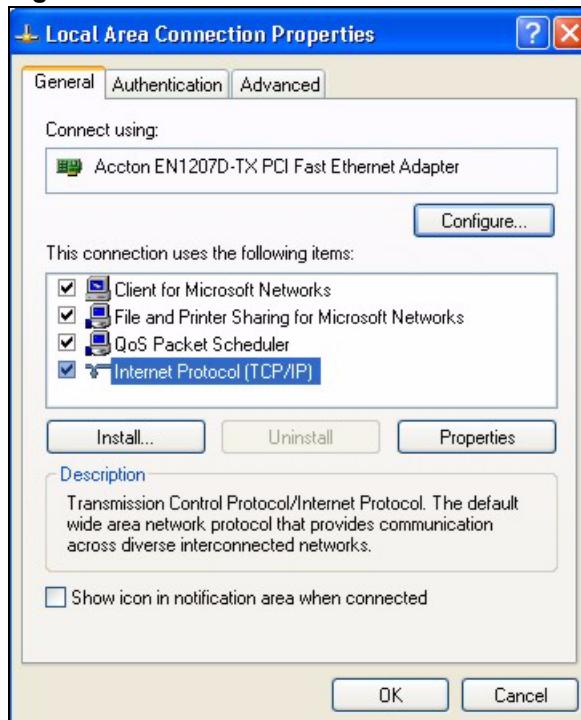
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 205 Windows XP: Control Panel

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

Figure 206 Windows XP: Control Panel: Network Connections: Properties

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

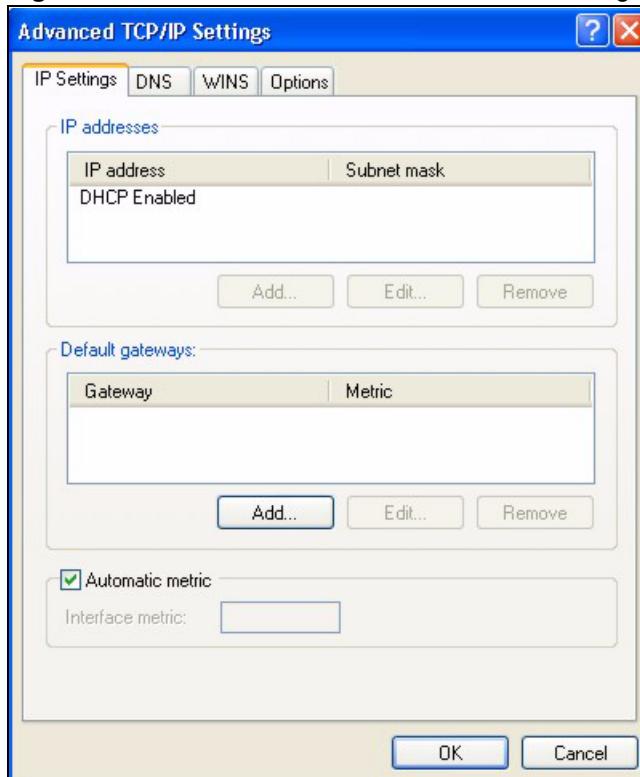
Figure 207 Windows XP: Local Area Connection Properties

- 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 208 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:

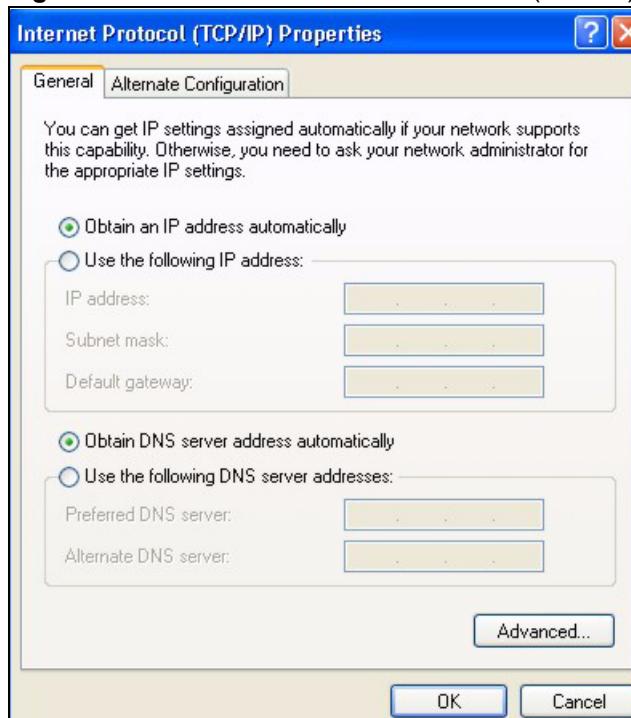
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP 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 209 Windows XP: Internet Protocol (TCP/IP) Properties



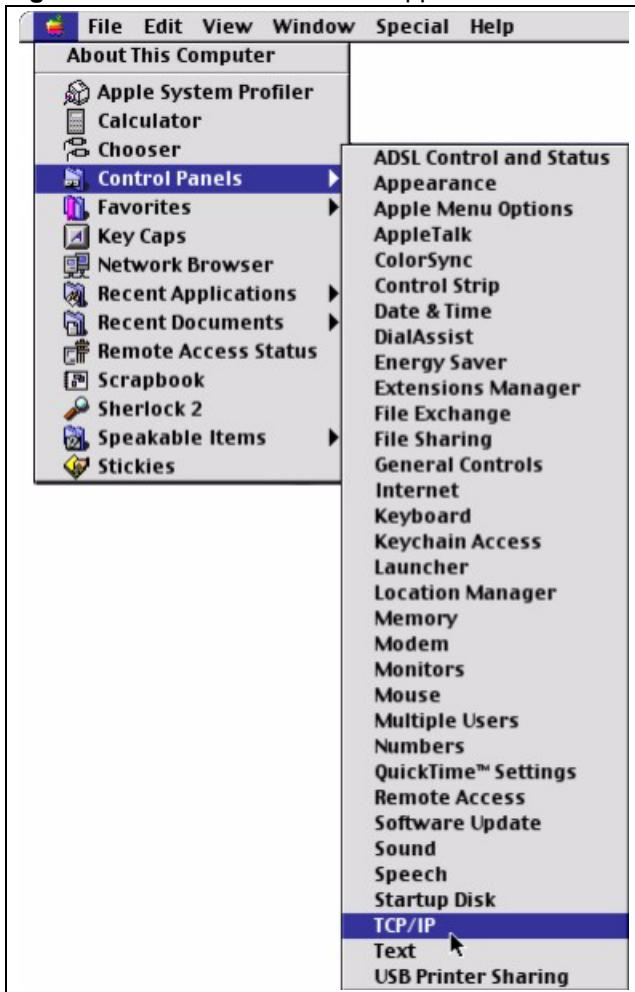
- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **OK** to close the **Local Area Connection Properties** window.
- 10 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

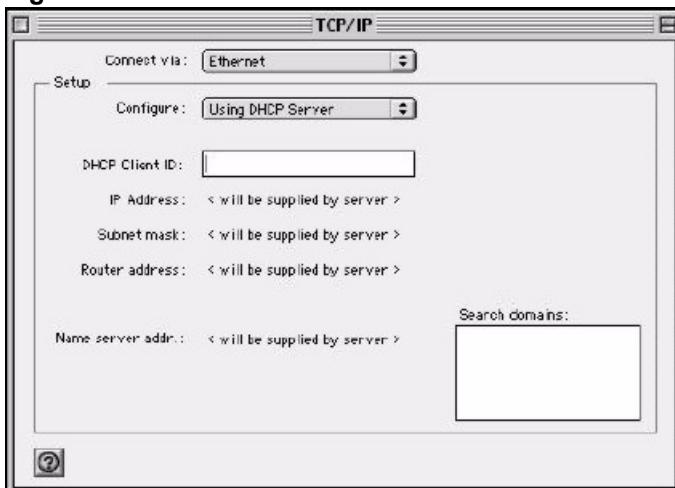
- 1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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

Figure 210 Macintosh OS 8/9: Apple Menu

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

Figure 211 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).

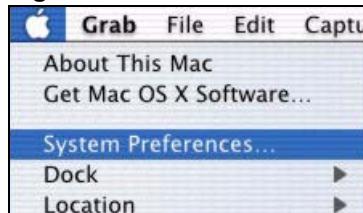
Verifying Settings

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.

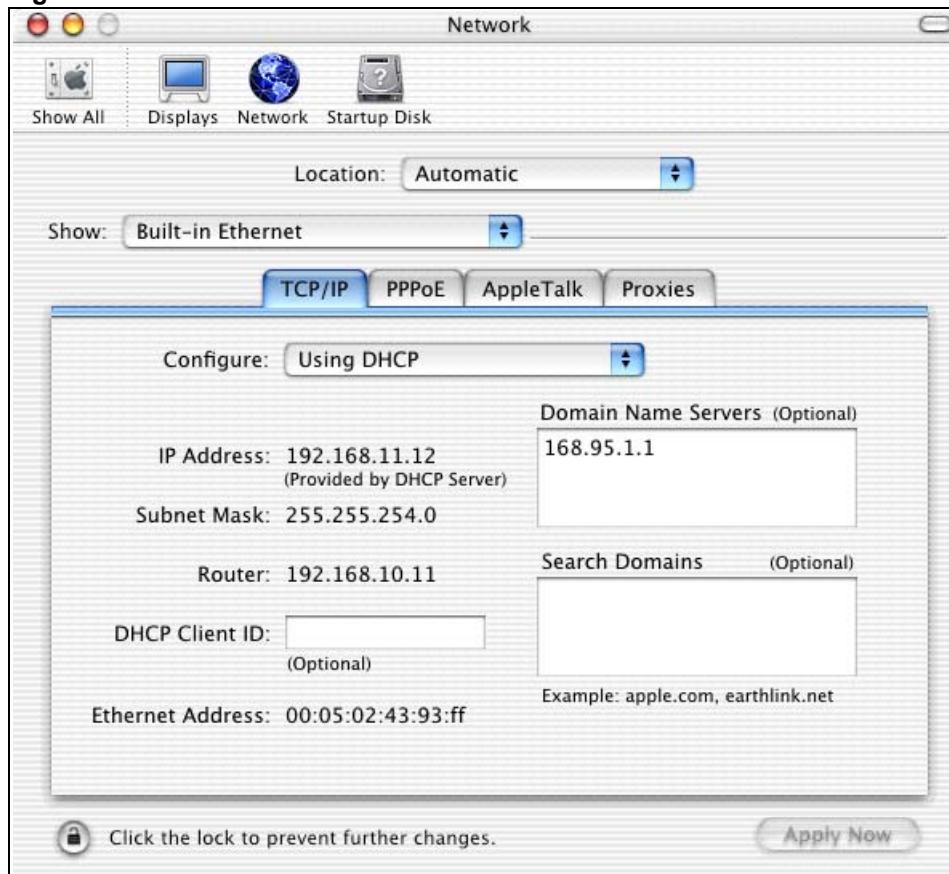
Figure 212 Macintosh OS X: Apple Menu



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 213 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 C

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 159 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 160 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 bits. If a bit in the subnet mask is “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 161 “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 162 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 163 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 164 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 165 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.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

Table 166 Subnet 1

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

Table 167 Subnet 2

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

Table 168 Subnet 3

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

Table 169 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 170 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 171 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 159 on page 381](#)) available for subnetting.

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

Table 172 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 D

About ADSL

Introduction to DSL

DSL (Digital Subscriber Line) technology enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line, but now everybody is searching for ways to get more bandwidth to improve access to the Web - hence DSL technologies.

There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). Asymmetrical services (ADSL) are suitable for Internet users because more information is usually downloaded than uploaded. For example, a simple button click in a web browser can start an extended download that includes graphics and text.

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds.

A DSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

ADSL Overview

Asynchronous Digital Subscriber Line (ADSL) technology provides high-speed data access across regular telephone or ISDN lines by making use of previously unused high-frequency bandwidth. ADSL is asymmetric in the sense that it provides a higher downstream data rate transfer (up to 8Mbps), than in the upstream transfer (up to 832 Kbps). Asymmetric operation is ideal for typical home and small office use where files and information are downloaded more frequently than uploaded.

Advantages of ADSL

- 1 ADSL provides a private (unlike cable telephone and modem services where the line is shared), dedicated and secure channel of communications between you and your service provider.

- 2** Because your line is dedicated (not shared), transmission speeds between you and the device to which you connect at your service provider are not affected by other users. With cable modems, transmission speeds drop significantly as more users go on-line because the line is shared.
- 3** ADSL can be "always on" (connected). This means that there is no time wasted dialing up the service several times a day and waiting to be connected; ADSL is on standby, ready for use whenever you need it.

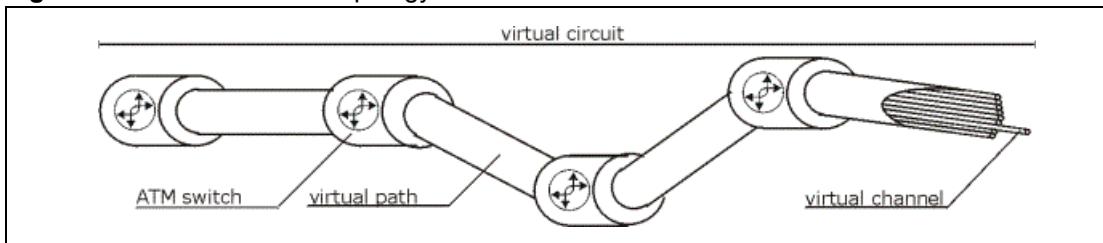
APPENDIX E

Virtual Circuit Topology

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

- Virtual Channel: Logical connections between ATM switches
- Virtual Path: A bundle of virtual channels
- Virtual Circuit: A series of virtual paths between circuit end points

Figure 214 Virtual Circuit Topology



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

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

Your ISP (Internet Service Provider) should supply you with VPI/VCI numbers.

APPENDIX F

Wireless LANs

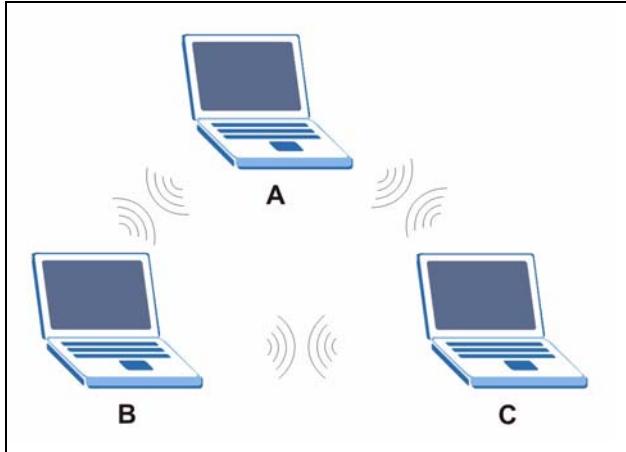
Wireless LAN Topologies

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

Ad-hoc Wireless LAN Configuration

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

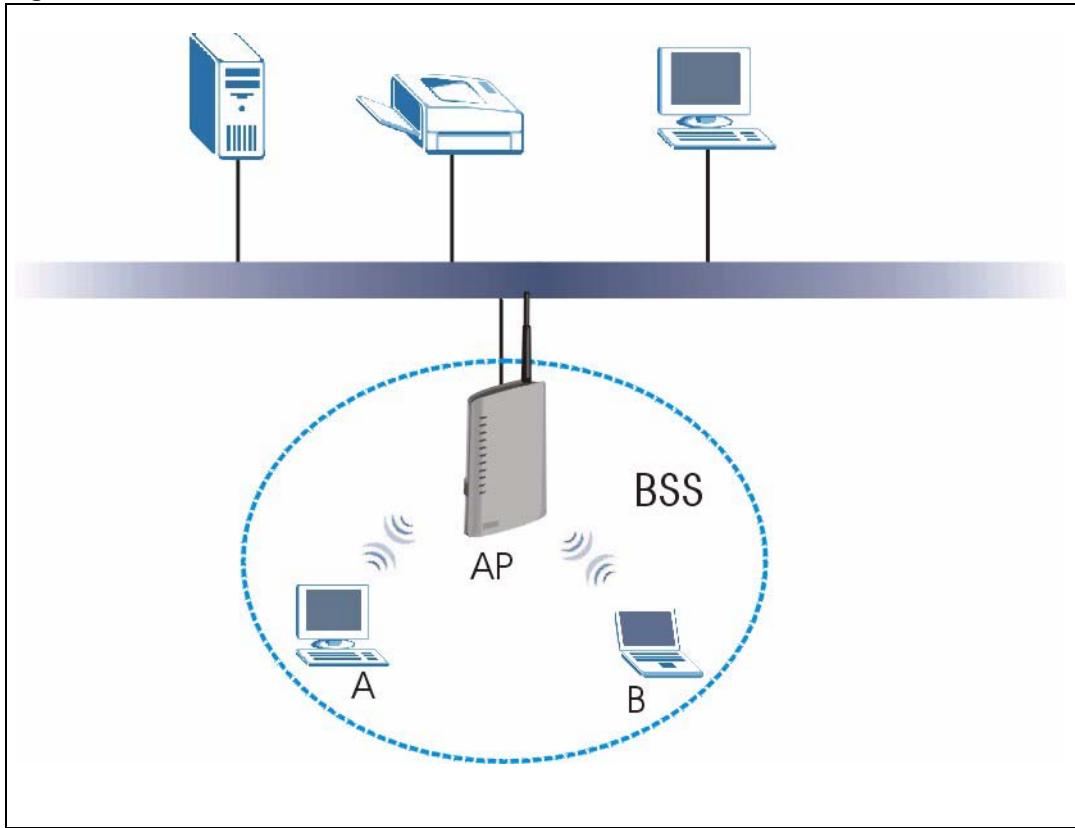
Figure 215 Peer-to-Peer Communication in an Ad-hoc Network



BSS

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

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

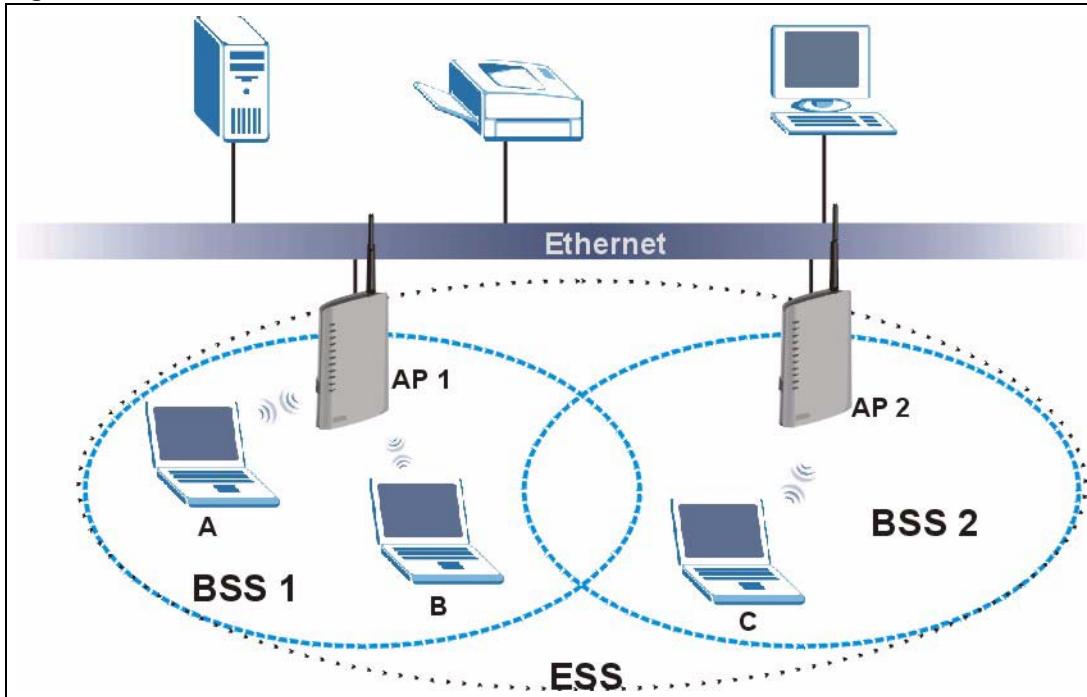
Figure 216 Basic Service Set

ESS

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

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

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

Figure 217 Infrastructure WLAN

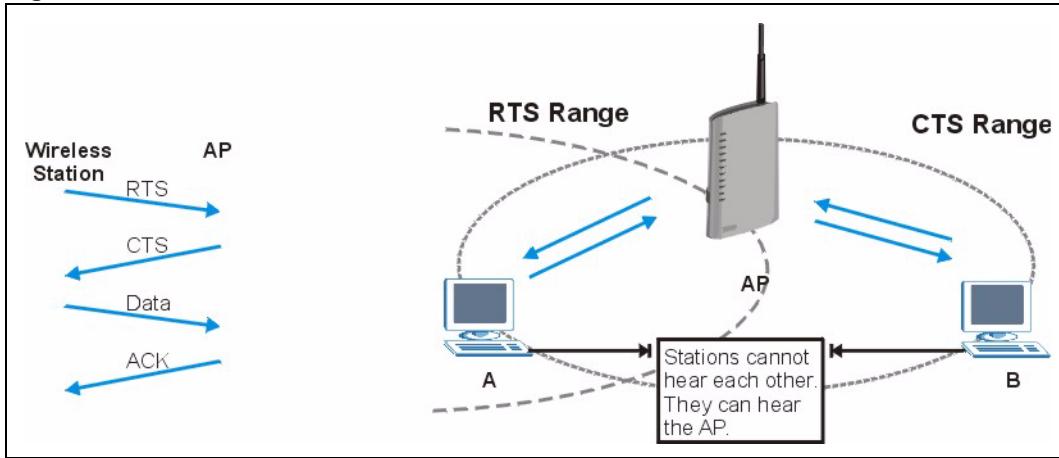
Channel

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

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

RTS/CTS

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

Figure 218 RTS/CTS

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

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

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

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

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

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

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

Fragmentation Threshold

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

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

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

Preamble Type

Preamble is used to signal that data is coming to the receiver. **Short** and **Long** refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support long preamble, but not all support short preamble.

Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.

Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.

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

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

IEEE 802.11g Wireless LAN

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

Table 173 IEEE 802.11g

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

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 174 Wireless Security Levels

Security Level	Security Type
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
	WPA2
Most Secure	

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

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

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

RADIUS

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

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

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

Types of RADIUS Messages

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

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

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

- Accounting-Request
Sent by the access point requesting accounting.
- Accounting-Response
Sent by the RADIUS server to indicate that it has started or stopped accounting.

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

Types of Authentication

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

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

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

LEAP

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

Dynamic WEP Key Exchange

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

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

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

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

Table 175 Comparison of EAP Authentication Types

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

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

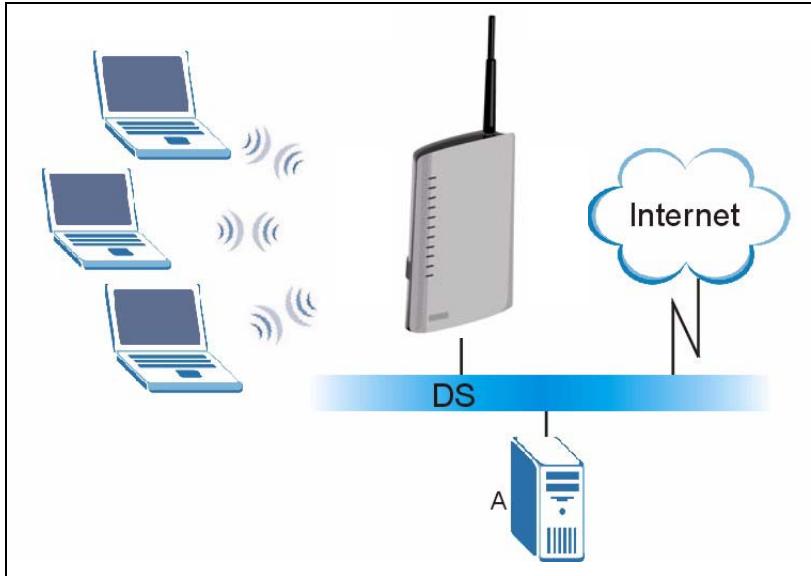
WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

- 3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

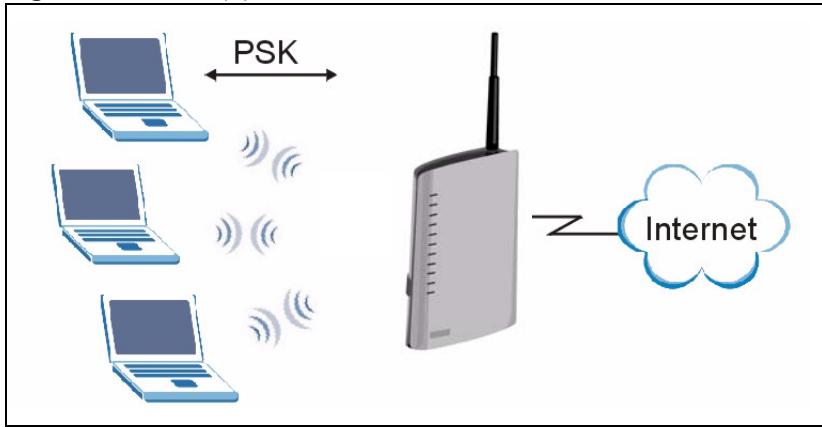
Figure 219 WPA(2) with RADIUS Application Example



27.5.1 WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
- 3 The AP and wireless clients use the pre-shared key to generate a common PMK (Pairwise Master Key).
- 4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 220 WPA(2)-PSK Authentication

Security Parameters Summary

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

Table 176 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

APPENDIX G

Common 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**. Please refer to RFC 1700 for further information about port numbers.
 - 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 177 Commonly Used Services

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

Table 177 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing 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.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
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).
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.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
RExec	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.

Table 177 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

APPENDIX H

Internal SPTGEN

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

Internal SPTGEN Overview

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

The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

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

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

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

Figure 221 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 221 on page 411](#)), 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 222 on page 412](#), 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 221 on page 411](#)).

Figure 222 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 223 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 224 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 225 Internal SPTGEN FTP Upload Example

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

Example Internal SPTGEN Menus

This section provides example Internal SPTGEN menus.

Table 178 Abbreviations Used in the Example Internal SPTGEN Screens Table

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

Table 179 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 180 Menu 3

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

Table 180 Menu 3

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

Table 180 Menu 3

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

Table 180 Menu 3

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

Table 181 Menu 4 Internet Access Setup

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

Table 181 Menu 4 Internet Access Setup (continued)

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

Table 182 Menu 12

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

Table 183 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(U DP)>	= 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(U DP)>	= 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(U DP)>	= 0
150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0(No) 1(Yes)>	= 0
150000018 =	SUA Server #5 Protocol	<0(All) 6(TCP) 17(U DP)>	= 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(U DP)>	= 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(U DP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0

Table 183 Menu 15 SUA Server Setup (continued)

1500000031 =	SUA Server #7 Local IP address		= 0.0.0.0
1500000032 =	SUA Server #8 Active	<0 (No) 1 (Yes) >	= 0
1500000033 =	SUA Server #8 Protocol	<0 (All) 6 (TCP) 17 (U DP) >	= 0
1500000034 =	SUA Server #8 Port Start		= 0
1500000035 =	SUA Server #8 Port End		= 0
1500000036 =	SUA Server #8 Local IP address		= 0.0.0.0
1500000037 =	SUA Server #9 Active	<0 (No) 1 (Yes) >	= 0
1500000038 =	SUA Server #9 Protocol	<0 (All) 6 (TCP) 17 (U DP) >	= 0
1500000039 =	SUA Server #9 Port Start		= 0
1500000040 =	SUA Server #9 Port End		= 0
1500000041 =	SUA Server #9 Local IP address		= 0.0.0.0
1500000042 =	SUA Server #10 Active	<0 (No) 1 (Yes) >	= 0
1500000043 =	SUA Server #10 Protocol	<0 (All) 6 (TCP) 17 (U DP) >	= 0
1500000044 =	SUA Server #10 Port Start		= 0
1500000045 =	SUA Server #10 Port End		= 0
1500000046 =	SUA Server #10 Local IP address		= 0.0.0.0
1500000047 =	SUA Server #11 Active	<0 (No) 1 (Yes) >	= 0
1500000048 =	SUA Server #11 Protocol	<0 (All) 6 (TCP) 17 (U DP) >	= 0
1500000049 =	SUA Server #11 Port Start		= 0
1500000050 =	SUA Server #11 Port End		= 0
1500000051 =	SUA Server #11 Local IP address		= 0.0.0.0
1500000052 =	SUA Server #12 Active	<0 (No) 1 (Yes) >	= 0
1500000053 =	SUA Server #12 Protocol	<0 (All) 6 (TCP) 17 (U DP) >	= 0
1500000054 =	SUA Server #12 Port Start		= 0
1500000055 =	SUA Server #12 Port End		= 0
1500000056 =	SUA Server #12 Local IP address		= 0.0.0.0

Table 184 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 set #1, rule #1			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1, Rule 1 Type	<2 (TCP/IP) >	= 2

Table 184 Menu 21.1 Filter Set #1 (continued)

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

Table 184 Menu 21.1 Filter Set #1 (continued)

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

Table 185 Menu 21.1 Filer Set #2,

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

Table 185 Menu 21.1 Filer Set #2, (continued)

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

Table 186 Menu 23 System Menus

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

Table 186 Menu 23 System Menus (continued)

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

Table 187 Menu 24.11 Remote Management Control

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

Table 187 Menu 24.11 Remote Management Control (continued)

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

Command Examples

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

Table 188 Command Examples

FIN	FN	PVA	INPUT
<i>/ci command (for annex a): wan adsl opencmd</i>			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(glite) 1(t1.413) 2(gdmt) 3(multimode)>	= 3
<i>/ci command (for annex B): wan adsl opencmd</i>			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(etsi) 1(normal) 2(gdmt) 3(multimode)>	= 3

APPENDIX I

Commands

This appendix describes how to use the commands to configure features that are not available through the web configurator. See the included disk or zyxel.com for more detailed information on these commands.

Accessing the Command Interpreter

Telnet to the ZyXEL Device and enter the password to use the 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. Use the `sys save` command at the end of a command configuration session to save all of your ZyXEL Device's parameters.

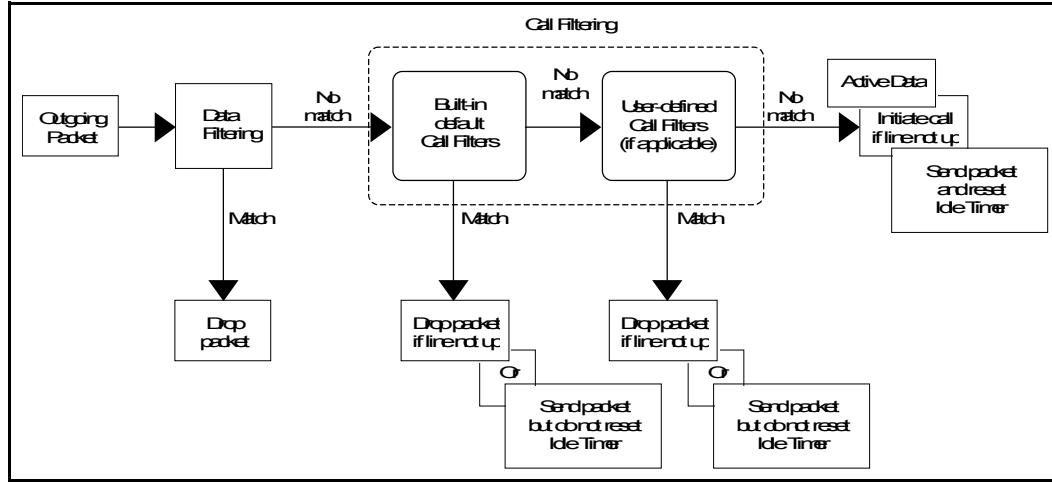
Filtering

Your ZyXEL Device uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

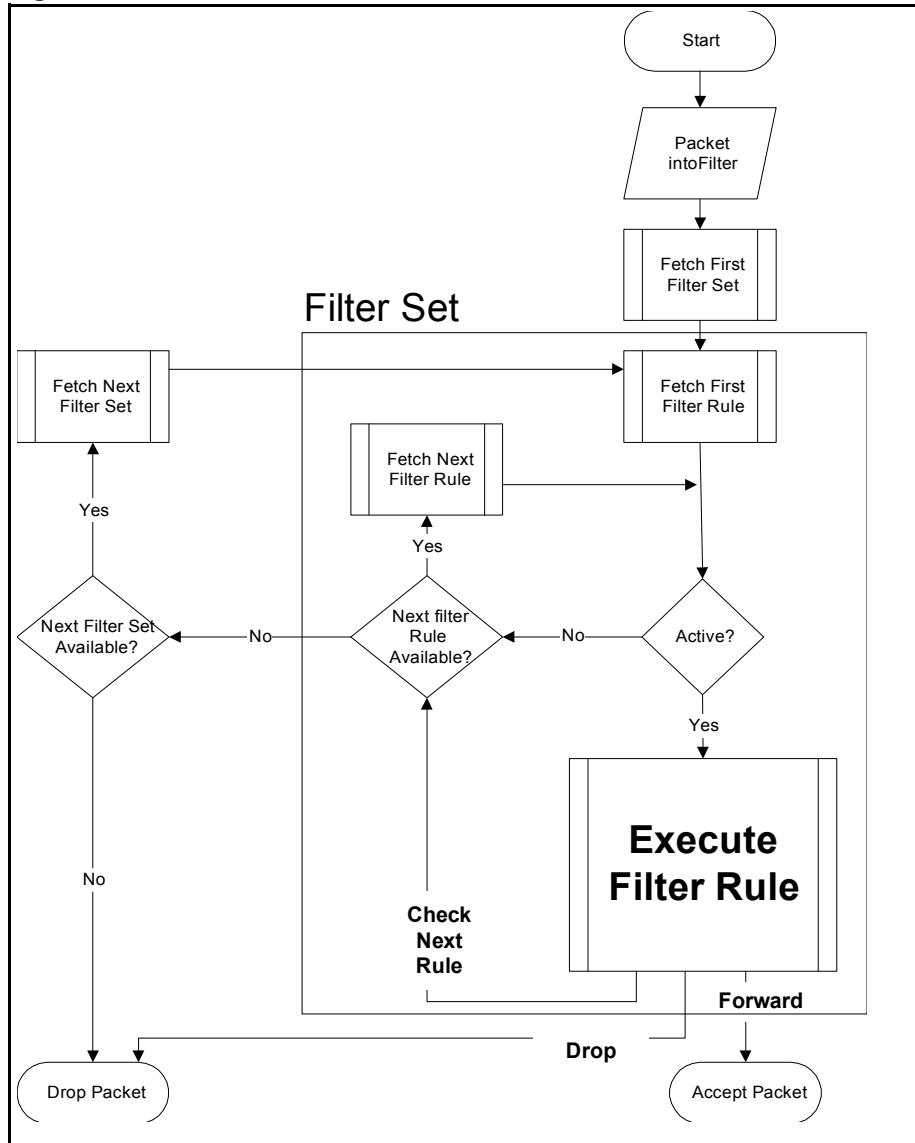
Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your ZyXEL Device has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your ZyXEL Device applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

Figure 226 Outgoing Packet Filtering Process



Two sets of factory filter rules have been configured to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

Figure 227 Filter Rule Process

You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your ZyXEL Device applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

The Filter Structure of the ZyXEL Device

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

Packet Filtering Vs. Firewall

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

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.

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.

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 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.

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.

Filter Commands

The following describes the filter commands.

Table 189 Filter Commands

COMMAND		DESCRIPTION
sys filter set	index [set#] [rule#]	Set the index number of a filter set rule. You must use this command first before you begin to configure the filter rule.
	name [set name]	Set the name of a filter set.
	type [tcpip generic]	Set the type of filter rule
	enable	Enable the rule.
	disable	Disable the rule.
	protocol [protocol #]	Set the protocol ID of the rule.
	sourceroute [yes no]	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If set to yes, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.
	destip [address] [subnet mask]	Set the destination IP address and subnet mask of the rule.
	destport [port#] [compare type = none equal notequal less greater]	Set the destination port and type of comparison to apply to the destination port in the packet. Possible comparisons are 0 (none), 1 (equal), 2 (not equal), 3 (less) or 4(greater).
	srcip [address] [subnet mask]	Set the source IP address and subnet mask.
	srcport [port#] [compare type = none equal not equal less greater]	Set the source port and type of comparison to apply to the destination port in the packet. Possible comparisons are 0 (none), 1 (equal), 2 (not equal), 3 (less) or 4(greater).
	tcpEstab [yes no]	This applies only when the IP Protocol field is 6, TCP. If Yes, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.
	more [yes no]	Set the more option to yes/no. If yes, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If the more option is yes, then action matched and action not matched will be N/A.
	log [type 0-3= none match notmatch both]	Set the log type (it could be 0-3 =none, match, not match, both).
	actmatch[type 0-2 = checknext forward drop]	Set the action for packets that match the filter rule.

Table 189 Filter Commands

COMMAND		DESCRIPTION
	actnomatch [type 0-2 = checknext forward drop]	Set the action for packets that do not match the filter rule.
	offset [#]	Set offset for the generic rule. Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.
	length [#]	Set the length for generic rule. Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.
	mask [#]	Set the mask for generic rule. Type the mask (in Hexadecimal) to apply to the data portion before comparison.
	value [(depend on length in hex)]	Set the value for generic rule. Type the value (in Hexadecimal) to compare with the data portion.
	clear	Clear the current filter set.
	save	Save the filter set parameters.
	display [set#][rule#]	Display filter set information. W/o any parameters, this displays buffer information.
	freememory	Discard changes.
lan	filter [incoming outgoing] [tcpip generic] [set#1] [set#2] [set#3] [set#4]	Set LAN filter to be incoming/outgoing or protocol /device and the filter set could be 1-12, 0 means empty. Example: Lan filter incoming tcpip 1 0 0 0
wan	node filter [incoming outgoing] [tcpip generic] [set #1] [set #2] [set #3] [set #4]	Set WAN filter, incoming or outgoing can be specified, and filter set can be 1-12, value 0 means empty.

WAN Call Schedules

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

Table 190 WAN Call Schedules

COMMAND		DESCRIPTION
wan callsch	index [set#]	Set the call schedule index #. You must apply this command first before you begin to configure a call schedule.
	name [set name]	Set the schedule name.
	active [Yes No]	Enable/Disable the schedule.
	startday [year] [month] [day]	Set the schedule start day.
	onceday [year] [month] [day]	Set the schedule to be used one time.
	weeklyday Sunday [1:active 0:inactive]	Set the schedule to recur weekly on Sundays.

Table 190 WAN Call Schedules

COMMAND		DESCRIPTION
	weeklyday Monday [1:active 0:inactive]	Set the schedule to recur weekly on Mondays.
	weeklyday Tuesday [1:active 0:inactive]	Set the schedule to recur weekly on Tuesdays.
	weeklyday Wednesday [1:active 0:inactive]	Set the schedule to recur weekly on Wednesdays.
	weeklyday Thursday [1:active 0:inactive]	Set the schedule to recur weekly on Thursdays.
	weeklyday Friday [1:active 0:inactive]	Set the schedule to recur weekly on Fridays.
	weeklyday Saturday [1:active 0:inactive]	Set the schedule to recur weekly on Saturdays.
	starttime [hour] [minute]	Set the schedule start time in hour and minute format.
	duration [hour] [minute]	Set the schedule duration time in hour and minute format.
	action [0:force on 1: force down 2: enable dial-on- demand 3: disable dial-on-demand]	Set the schedule's action. Force on means that the connection is maintained whether or not there is a demand call on the line and will persist for the specified duration. Force down means that the connection is blocked whether or not there is a demand call on the line. Enable dial-on-demand means that this schedule permits a demand call on the line. Disable dial-on-demand means that this schedule prevents a demand call on the line.
	display	Show the current call schedule set.
	save	Save the current call schedule set.
	freememory	Free the current call schedule set.
	clear	Clear the call schedule set.

Index

A

AAL5 **364**
 Abs **171**
 ACK Message **166**
 Address Assignment **119**
 Address Resolution Protocol (ARP) **122**
 ADSL Standards **40**
 ADSL2 **364**
 Advanced Encryption Standard **402**
 AH **237**
 AH Protocol **241**
 ALG **43, 171**
 Alternative Subnet Mask Notation **383**
 Analysis-by-Synthesis **171**
 ANSI T1.413 **364**
 Antenna **363**
 Any IP **41, 121**
 How it works **122**
 note **122**
 Any IP Setup **124**
 AP (access point) **395**
 Application Layer Gateway **43, 171**
 Application-level Firewalls **200**
 Applications
 Internet access **46**
 Asynchronous Transfer Mode **349**
 ATM AAL5 **364**
 ATM Adaptation Layer 5 (AAL5) **87**
 ATM Adaptation Layer type 5 **364**
 ATM Loopback Test **349**
 ATM Status **349**
 Attack Alert **229**
 Attack Types **204**
 Authentication Header **237, 241**
 Auto Firmware Upgrade **41, 198**
 Auto-crossover **40**
 Automatic Log Out **55**
 Auto-negotiating Rate Adaptation **364**
 Auto-negotiation **40**
 Auto-provisioning **41, 198**

B

Backup **337**
 Backup Type **101**
 Bandwidth Management **273**
 Bandwidth Manager Class Configuration **279**
 Bandwidth Manager Monitor **283**
 Bandwidth Manager Summary **278**
 Basic wireless security **73**
 Blocking Time **228, 229**
 Brute-force Attack, **203**
 BSS **393**
 BW Budget **280**
 BYE Request **166**

C

CA **400**
 Call Filtering **427**
 Call Filters
 Built-in **428**
 User-defined **428**
 Call Hold **184, 186**
 Call Scheduling **432**
 Call Service Mode **184, 186**
 Call Transfer **185, 186**
 Call Waiting **185, 186**
 Caller ID **366**
 Capture All Logs **350**
 CBR (Continuous Bit Rate) **96, 100**
 CCK **45**
 Certificate Authority **400**
 Certifications **4**
 Notice 1 **4**
 viewing **4**
 Change Password at Login **54**
 Channel **395**
 Interference **395**
 Channel ID **135**
 Checking the Device's IP Address **197**
 Client-server Protocol **166**
 CNG **366**
 Codec **171, 366**

Coder/Decoder **171**
Comfort Noise Generation **43, 179, 366**
Complementary Code Keying Modulation **45**
Computer **38**
Configuration **107, 118**
Configuration File **333**
Contact Information **8**
Content Filtering **42, 231**
 Categories **231**
 Schedule **232**
 Trusted computers **233**
 URL keyword blocking **231**
Content filtering **231**
Copyright **3**
CTS (Clear to Send) **396**
Custom Ports
 Creating/Editing **223**
Customer Support **8**
Customized Services **222**

DoS **201**
 Basics **201**
 Types **202**
DoS (Denial of Service) **41**
DoS attacks, types of **202**
DQPSK **45**
DSL (Digital Subscriber Line) **389**
DSL Line Status **349**
DSL line, reinitialize **350**
DSLAM (Digital Subscriber Line Access Multiplexer) **46**
DTMF **172**
DTMF Detection and Generation **366**
Dual-Tone MultiFrequency **172**
Duplex **40**
Dynamic DNS **44, 285**
Dynamic Host Configuration Protocol **44**
Dynamic Jitter Buffer **42, 366**
Dynamic Secure Gateway Address **243**
Dynamic WEP Key Exchange **401**
DYNDNS Wildcard **285**

D

Data Confidentiality **236**
Data Filtering **427**
Data Integrity **236**
Data Origin Authentication **236**
DBPSK **45**
Decoder **171**
Default **339**
Default LAN IP Address **53**
Denial of Service **200, 201, 228**
Destination Address **213**
DH **256**
DHCP **44, 107, 118, 119, 285, 313**
DHCP Client **44**
DHCP Relay **44**
DHCP Server **44**
DHCP Table **107**
Diagnostic **347**
Differential Binary Phase Shift Keyed Modulation **45**
Differential Quadrature Phase Shift Keying Modulation
 45
Diffie-Hellman Key Groups **256**
Disclaimer **3**
DNS **297**
DNS Server
 For VPN Host **247**
Domain Name **119, 313**
Domain Name System **118**

E

EAP Authentication **400**
EAP-MD5 **364**
Echo Cancellation **43, 179, 366**
E-mail **150**
 Log Example **323**
Emergency Numbers **179**
Encapsulated Routing Link Protocol (ENET ENCAP) **87**
Encapsulating Security Payload **237**
Encapsulation **87, 237**
 ENET ENCAP **87**
 PPP over Ethernet **87**
 PPPoA **87**
 RFC 1483 **88**
Encapsulation Security Payload **241**
Encryption **235, 402**
ESP Protocol **237, 241**
ESS **394**
Europe Type Call Service Mode **184**
Extended Service Set **394**
Extended Service Set IDentification **135**
Extended wireless security **73**
External Antenna **45**
External RADIUS **364**

F

F4/F5 OAM [364](#)
 Fairness-based Scheduler [274](#)
 FCC Interference Statement [4](#)
 Filename Conventions [333, 334](#)

Filter [427](#)
 Filter Structure [429](#)
 Filter Rule Process [429](#)
 Filtering Process
 Outgoing Packets [428](#)

Firewall
 Access Methods [211](#)
 Address Type [221](#)
 Alerts [214](#)
 Creating/Editing Rules [219](#)
 Custom Ports [222](#)
 Enabling [216](#)
 Firewall Vs Filters [430](#)
 Guidelines For Enhancing Security [209](#)
 Introduction [200](#)
 LAN to WAN Rules [214](#)
 Policies [211](#)
 Rule Checklist [212](#)
 Rule Logic [212](#)
 Rule Security Ramifications [212](#)
 Services [227](#)
 Types [199](#)
 When To Use [430](#)

Firmware [333](#)
 upload [334](#)
 upload error [336](#)

Flash Key [184](#)
 Flashing [184](#)
 Fragmentation Threshold [396](#)
 Fragmentation threshold [396](#)
 Frame Relay [46](#)
 Frequency Range [364](#)
 FTP [158, 289, 293](#)
 File Upload [343](#)
 FTP Restrictions [289, 334](#)
 Full Rate [51](#)
 Full-duplex [40](#)

G
 G.168 [43, 179, 366](#)
 G.711 [171, 366](#)
 G.729 [171, 366](#)
 G.992.1 [364](#)
 G.992.3 [364](#)

G.992.4 [364](#)
 G.992.5 [364](#)
 G.dmt [364](#)
 G.lite [364](#)
 G992.2 [364](#)
 General Setup [313](#)
 General wireless LAN screen [134](#)
 Graphical User Interface (GUI) [40](#)
 Graphics Icons [38](#)
 Graphics Icons Key [38](#)

H

H.323 Passthrough [366](#)
 Half-duplex [40](#)
 Half-Open Sessions [228](#)
 Hidden node [395](#)
 Host [314](#)
 Host IDs [381](#)
 Housing [44](#)
 HTTP (Hypertext Transfer Protocol) [201, 202, 334](#)
 HTTP (hypertext Transfer Protocol) [200](#)
 Humidity [363](#)
 Hybrid, Waveform Codec [171](#)

I

IANA [120](#)
 IANA (Internet Assigned Number Authority) [222](#)
 IBSS [393](#)
 ICMP echo [204](#)
 Icons Key [38](#)
 ID Type and Content [247](#)
 IEEE 802.11g [45, 397](#)
 IEEE 802.11g Data Rates [45](#)
 IEEE 802.11g Modulation [45](#)
 IEEE 802.11g Wireless LAN [45](#)
 IEEE 802.11i [45](#)
 IEEE 802.1Q VLAN [177](#)
 IGMP [121](#)
 IGMP Proxy [364](#)
 IGMP v1 [364](#)
 IGMP v2 [364](#)
 IKE Phases [254](#)
 Independent Basic Service Set [393](#)
 Initialization Vector (IV) [402](#)

Inside Header [238](#)

Install UPnP [303](#)

Windows Me [303](#)

Windows XP [305](#)

Integrated Access Device [39](#)

Internal Calls [197](#)

Internal SPTGEN [411](#)

FTP Upload Example [413](#)

Points to Remember [412](#)

Text File [411](#)

Internet Access [40, 46](#)

Internet access [61](#)

Internet Access Setup [352](#)

Internet access wizard setup [61](#)

Internet Assigned Numbers AuthoritySee IANA [120](#)

Internet Control Message Protocol (ICMP) [203](#)

Internet Key Exchange [254](#)

Internet Protocol Security [235](#)

Internet Telephony Service Provider [46](#)

IP Address [107, 119, 158, 159, 160](#)

IP Address Assignment [88](#)

ENET ENCAP [89](#)

PPPoA or PPPoE [88](#)

RFC 1483 [89](#)

IP Addressing [381](#)

IP Alias [44](#)

IP Classes [381](#)

IP Multicasting [364](#)

IP Policy Routing (IPPR) [44](#)

IP Pool [125](#)

IP Pool Setup [118](#)

IP protocol type [227](#)

IP Spoofing [202, 205](#)

IP to IP Calls [47](#)

IPSec [235](#)

IPSec Algorithms [237, 241](#)

IPSec and NAT [238](#)

IPSec Architecture [237](#)

IPSec Passthrough [365](#)

IPSec standard [42](#)

ISDN (Integrated Services Digital Network) [39, 179](#)

ITSP [46](#)

ITU-T [179](#)

ITU-T G.992.1 [349](#)

J

Jitter Buffer [42](#)

K

Keep Alive [245](#)

Key Fields For Configuring Rules [213](#)

L

LAN Setup [87, 117](#)

LAN TCP/IP [119](#)

LAN to WAN Rules [214](#)

LAND [202, 203](#)

Log Out [55](#)

Logs [319](#)

M

MAC Address Filter Action [146](#)

MAC Address Filtering [145](#)

MAC Filter [145](#)

Management Information Base (MIB) [295](#)

Maximize Bandwidth Usage [275](#)

Maximum Burst Size (MBS) [91, 96, 100](#)

Max-incomplete High [228](#)

Max-incomplete Low [228](#)

Media Bandwidth Management [42](#)

Message Integrity Check (MIC) [402](#)

Metric [90](#)

Modem [38](#)

Multicast [121](#)

Multimedia [165](#)

Multiple PVC Support [44](#)

Multiple SIP Accounts [43](#)

Multiple Voice Channels [43](#)

Multiplexing [88](#)

LLC-based [88](#)

VC-based [88](#)

Multiprotocol Encapsulation [88](#)

My IP Address [242](#)

N

Nailed-Up Connection [89](#)

NAT [119, 158, 159](#)

Address mapping rule [163](#)

Application **155**
 Definitions **153**
 How it works **154**
 Mapping Types **155**
 What it does **154**
 What NAT does **154**
 NAT (Network Address Translation) **153**
 NAT mode **157**
 NAT Sessions **365**
 NAT Traversal **301**
 NAT traversal **246**
 Negotiation Mode **255**
 NetBIOS commands **204**
 Network Address Translation (NAT) **42**
 Notebook Computer **38**

O

OAM **364**
 OFDM **45**
 OK Response **166**
 One-Minute High **228**
 Operation Humidity **363**
 Operation Temperature **363**
 Orthogonal Frequency Division Multiplexing Modulation
45
 Outside Header **238**

P

Packet Filtering **430**
 When to use **430**
 Packet Filtering Firewalls **199**
 Pairwise Master Key (PMK) **402, 404**
 PCM **171**
 Peak Cell Rate (PCR) **90, 96, 100**
 Peer to Peer Calls **47**
 Peer-to-peer Calls **47**
 Perfect Forward Secrecy **256**
 Permanent Virtual Circuits **364**
 PFS **256**
 Phone **178**
 Ping of Death **202**
 Point to Point **389**
 Point to Point Calls **47, 366**
 Point to Point Protocol over ATM Adaptation Layer 5
 (AAL5) **87**

POP3 **201, 202**
 Port Forwarding **365**
 Power Adapter **366**
 Power Adapter Specifications **366**
 Power Specification **363**
 PPP (Point-to-Point Protocol) Link Layer Protocol **364**
 PPP over ATM AAL5 **364**
 PPP over Ethernet **364**
 PPP session over Ethernet (PPP over Ethernet, RFC
 2516) **87**
 PPPoE **89**
 Benefits **89**
 PPPoE (Point-to-Point Protocol over Ethernet) **43, 89**
 Preamble Mode **397**
 Pre-Shared Key **249**
 Priorities **147, 277**
 Priority **280**
 Priority-based Scheduler **274**
 PSTN Call Setup Signaling **172**
 Public Switched Telephone Network **39**
 Pulse Code Modulation **171**
 Pulse Dialing **172**
 PVC (Permanent Virtual Circuit) **87**
 PVCs **364**

Q

Quality of Service (QoS) **43, 177**
 Quick Dialing **366**
 Quick Start Guide **37, 53**

R

RADIUS **364, 399**
 Shared Secret Key **400**
 RADIUS Message Types **399**
 RADIUS Messages **399**
 Reach-Extended ADSL **364**
 Real Time E-mail Alerts **365**
 Real time Transport Protocol **171**
 Reinitialize the ADSL line **350**
 Related Documentation **37**
 Remote Management and NAT **290**
 Remote Management Limitations **289**
 REN **42**
 Reports and Logs **365**

Required Bandwidth **171**
Reset ADSL Line **350**
Reset Button **55**
Resetting Your Device **55**
Restore **338**
Restore Configuration **343**
RF (Radio Frequency) **45**
RFC 1483 **88, 364**
RFC 1631 **153**
RFC 1889 **171, 366**
RFC 1890 **366**
RFC 2327 **366**
RFC 2364 **364**
RFC 2516 **43, 364**
RFC 2684 **364**
RFC 3261 **366**
Ringer Equivalence Number **42**
RIP
 See Routing Information Protocol **120**
Romfile **333**
Router **38**
Routing Information Protocol **120**
 Direction **120**
 Version **120**
RTCP **366**
RTP **171, 366**
RTS (Request To Send) **396**
RTS Threshold **395, 396**
Rules **214**
 Checklist **212**
 Key Fields **213**
 LAN to WAN **214**
 Logic **212**
 Predefined Services **227**

S

SA **235**
Safety Warnings **6**
Saving the State **205**
Scheduler **274**
SDP **366**
Seamless Rate Adaptation **364**
Secure Gateway Address **243**
Security Association **235**
Security In General **209**
Security Parameter Index **259**
Security Parameters **405**
Security Ramifications **212**

Server **38, 156, 316**
Service **213**
Service Set **135**
Service Type **223, 352**
Services **158**
Session Description Protocol **366**
Session Initiating Protocol **366**
Session Initiation Protocol **165**
Silence Suppression **43, 179, 366**
Single User Account (SUA) **46**
SIP **165**
SIP Account **165**
SIP Accounts **43**
SIP ALG **43, 171**
SIP ALG Passthrough **365**
SIP Application Layer Gateway **43, 171**
SIP Call Progression **166**
SIP Client **166**
SIP Identities **165**
SIP INVITE Request **166**
SIP Number **78, 165**
SIP Proxy Server **167**
SIP Redirect Server **168**
SIP Register Server **169**
SIP Server Address **78**
SIP Servers **166**
SIP Service Domain **78, 166**
SIP URI **165**
SIP User Agent **167**
SIP Version 2 **366**
SIP, Authentication Password **79**
SIP, Authentication User ID **78**
SMTP Error Messages **323**
Smurf **203, 204**
SNMP **294, 364**
 Manager **295**
 MIBs **295**
SOHO (Small Office/Home Office) **46**
Sound Quality **171**
Source Address **213**
Speed Dial **189, 197**
SPI **259**
Splitters **51**
SPTGEN **366**
SRA **364**
Stateful Inspection **41, 199, 200, 205, 206**
 on Your ZyXEL Device **207**
 Process **206**
Stateful Packet Inspection **365**
Static Route **269**

Storage Humidity **363**
 Storage Temperature **363**
SUA 156
 SUA (Single User Account) **156**
 SUA vs NAT **156**
 Subnet Mask **119, 221**
 Subnet Masks **382**
 Subnetting **382**
 Supplementary Phone Services (ISDN) **187**
 Supplementary Phone Services (PSTN) **183**
 Supplementary Services **183**
 Supporting Disk **37**
 Sustain Cell Rate (SCR) **96, 100**
 Sustained Cell Rate (SCR) **90**
 Switch **38**
 SYN Flood **202, 203**
 SYN-ACK **203**
 Syntax Conventions **37**
 Syslog **226**
 System Name **314**
 System Parameter Table Generator **411**
 System Timeout **290**

T

TCP Maximum Incomplete **228, 229**
 TCP Security **207**
 TCP/IP **201, 202**
 Teardrop **202**
 Telephone **38**
 Telnet **291**
 Temperature **363**
 Temporal Key Integrity Protocol (TKIP) **402**
 Text File Format **411**
 TFTP
 File Upload **344**
 TFTP and FTP over WAN **334**
 TFTP Restrictions **289, 334**
 Three-Way Conference **185, 187**
 Three-Way Handshake **203**
 Threshold Values **227**
 TLS **364**
 ToS **177**
 Traceroute **205**
 Trademarks **3**
 Traffic redirect **102**
 Traffic shaping **90**
 Transparent Bridging **364**

Transport Mode **238**
 Triangle **214**
 Triangle Route Solutions **215**
 TTLS **364**
 Tunnel Mode **238**
 Type Of Service **177**

U

UBR (Unspecified Bit Rate) **96, 100**
 UDP/ICMP Security **208**
 Uniform Resource Identifier **165**
 Universal Plug and Play **301**
 Application **301**
 Security issues **302**
 Universal Plug and Play (UPnP) **43**
 Universal Plug and Play Forum **302**
 Upload Firmware **343**
 UPnP **301**
 Upper Layer Protocols **207, 208**
 USA Type Call Service Mode **186**
 User Authentication **403**
 User Name **286**
 Using Speed Dial **197**

V

VAD **43, 179, 366**
 VBR (Variable Bit Rate) **96, 100**
 Virtual Channel Identifier (VCI) **88**
 Virtual Circuit (VC) **88**
 Virtual Local Area Network **177**
 Virtual Path Identifier (VPI) **88**
 Virtual Private Network **235**
 VLAN **177**
 VLAN Group **177**
 VLAN ID **177**
 VLAN ID Tags **177**
 Voice Activity Detection **43, 179, 366**
 Voice Channels **43**
 Voice Coding **171**
 VoIP **165**
 VoIP Standards Compliance **43**
 VPI & VCI **88**
 VPN **235**
 VPN Applications **236**

W

WAN (Wide Area Network) **87**
WAN backup **100**
WAN to LAN Rules **214**
Warranty
 Note **7**
Waveform Codec **171**
Web **290**
Web Configurator **53, 209, 213**
WEP (Wired Equivalent Privacy) **45**
WEP Encryption **137**
WEP encryption **135**
Wi-Fi Multimedia QoS **147**
Wi-Fi Protected Access **402**
Wi-Fi Protected Access (WPA) **45**
Wireless Client WPA Suplicants **403**
Wireless LAN MAC Address Filtering **45**
Wireless security **398**
WLAN
 Interference **395**
 Security parameters **405**
WPA **402**
WPA2 **402**
WPA2-Pre-Shared Key **402**
WPA2-PSK **402**
WPA-PSK **402**
WWW **150**

Z

Zero Configuration Internet Access **41**
Zero configuration Internet access **92**
ZyNOS **334**
ZyNOS (ZyXEL Network Operating System) **333**
ZyNOS F/W Version **334**
ZyXEL's Firewall **200**