

P-870HW-I Series

802.11g Wireless VDSL2 4-port Gateway

User's Guide

Version 3.50

8/2006

Edition 1

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

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

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

Certifications

Federal Communications Commission (FCC) Interference Statement

The 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 device 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 residential installation. This device 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. However, there is no guarantee that interference will not occur in a particular installation.

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

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



FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

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

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。減少電磁波影響，請妥適使用。

Notices

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

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

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

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

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

Viewing Certifications

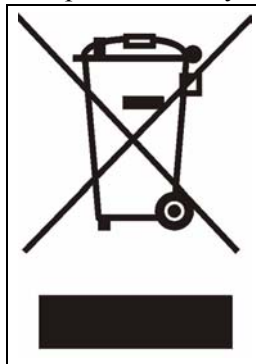
- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

Safety Warnings

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

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- 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 should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- **CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.** Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- **Antenna Warning!** This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

This product is recyclable. Dispose of it properly.



ZyXEL Limited Warranty

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

Note

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

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

Registration

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

Customer Support

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

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

METHOD	SUPPORT E-MAIL	TELEPHONE	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
	sales@zyxel.co.cr	+506-2015098	ftp.zyxel.co.cr	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	

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

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

Table of Contents

Copyright	3
Certifications	4
Safety Warnings	6
ZyXEL Limited Warranty	8
Customer Support	9
Table of Contents	11
List of Figures	23
List of Tables	31
Preface	37
Chapter 1	
Getting To Know Your ZyXEL Device	39
1.1 Introducing the ZyXEL Device	39
1.2 Features	39
1.2.1 Wireless Features	41
1.3 Application	42
1.3.1 Protected Internet Access	42
1.3.2 Management Server	43
1.4 LEDs	43
1.5 Splitters and Microfilters	44
1.5.1 Connecting a POTS Splitter	44
1.5.2 Telephone Microfilters	45
Chapter 2	
Introducing the Web Configurator	47
2.1 Web Configurator Overview	47
2.2 Accessing the Web Configurator	47
2.3 Navigating the Web Configurator	49
2.4 Resetting the ZyXEL Device	53
Chapter 3	
Connection Wizard	55
3.1 Main Wizard Screen	55

3.2 Welcome Screen	56
3.3 System Information Screen	56
3.4 Wireless LAN Screen	57
3.5 Wireless Security Screens	59
3.5.1 Wireless Security: None	59
3.5.2 Wireless Security: Basic Security Screen 1	59
3.5.3 Wireless Security: Basic Security Screen 2	60
3.5.4 Wireless Security: Auto	61
3.5.5 Wireless Security: Extend (WPA-PSK) Security Screen 1	62
3.5.6 Wireless Security: Extend (WPA-PSK) Security Screen 2	63
3.5.7 Wireless Security: Extend (WPA2-PSK) Security Screen 1	64
3.5.8 Wireless Security: Extend (WPA2-PSK) Security Screen 2	66
3.6 Auto-Detection Screen	66
3.7 ISP Parameters Screen	67
3.7.1 ISP Parameters: Ethernet Screen	67
3.7.2 ISP Parameters: PPPoE Screen	68
3.8 IP Address Type Screen	69
3.9 Static IP Address Settings Screen	70
3.9.1 Static IP Address Settings: Ethernet Screen	70
3.9.2 ISP Parameters: PPPoE Screen	71
3.10 MAC Address Screen	72
3.11 Internet Configuration Screen	74
3.12 Auto-Detection Screen	74
3.13 Congratulations Screen	75
Chapter 4	
Bandwidth Management Wizard	77
4.1 Main Wizard Screen	77
4.2 Welcome Screen	78
4.3 General Information Screen	79
4.4 Services Setup Screen	81
4.5 Priority Setup Screen	82
4.6 Congratulations Screen	83
Chapter 5	
Status Screen	85
5.1 Status Screen	85
5.1.1 Status: BW MGMT Monitor	87
5.1.2 Status: DHCP Table	88
5.1.3 Status: Packet Statistics	89
5.1.4 Status: WLAN Station Status	90

Chapter 6	
Wireless LAN	93
6.1 Wireless Network Overview	93
6.2 Wireless Security Overview	94
6.2.1 SSID	94
6.2.2 MAC Address Filter	94
6.2.3 User Authentication	94
6.2.4 Encryption	95
6.2.5 One-Touch Intelligent Security Technology (OTIST)	96
6.3 Wireless Performance Overview	96
6.3.1 Quality of Service (QoS)	96
6.4 General Wireless LAN Screen	96
6.4.1 General Wireless LAN Screen: No Security	97
6.4.2 General Wireless LAN Screen: Static WEP	98
6.4.3 General Wireless LAN Screen: WPA-PSK	99
6.4.4 General Wireless LAN Screen: WPA	100
6.4.5 General Wireless LAN Screen: 802.1x + Dynamic WEP	101
6.4.6 General Wireless LAN Screen: 802.1x + Static WEP	103
6.4.7 General Wireless LAN Screen: 802.1x + No WEP	104
6.4.8 General Wireless LAN Screen: WPA2-PSK	106
6.4.9 General Wireless LAN Screen: WPA2	107
6.5 OTIST Screen	108
6.5.1 Notes on OTIST	111
6.6 MAC Filter Screen	111
6.7 Advanced Wireless LAN Screen	113
Chapter 7	
WAN	119
7.1 WAN Overview	119
7.1.1 Nailed-Up Connection (PPP)	119
7.1.2 Metric	119
7.2 Internet Connection Screens	120
7.2.1 Internet Connection Screen: Ethernet	120
7.2.2 Internet Connection Screen: PPP over Ethernet (PPPoE)	121
7.3 Advanced WAN Screen	123
7.4 Traffic Redirect Screen	124
Chapter 8	
LAN	127
8.1 LAN Overview	127
8.1.1 IP Address and Subnet Mask	127
8.1.2 RIP Setup	127
8.1.3 Multicast	128

8.1.4 LAN IP Alias	128
8.2 LAN IP Screen	129
8.3 LAN IP Alias Screen	129
8.4 Advanced LAN Screen	131
Chapter 9	
DHCP Server	133
9.1 DHCP Overview	133
9.2 General DHCP Screen	134
9.3 Static DHCP Screen	135
9.4 Client List Screen	136
Chapter 10	
NAT	137
10.1 NAT Overview	137
10.1.1 Port Forwarding: Services and Port Numbers	137
10.1.2 Trigger Port Forwarding	138
10.1.2.1 Trigger Port Forwarding Example	138
10.1.2.2 Two Points To Remember About Trigger Ports	139
10.2 General NAT Screen	139
10.3 Port Forwarding Screen	140
10.3.1 Port Forwarding Edit Screen	141
10.4 Trigger Port Screen	142
10.5 Address Mapping Screen	143
10.5.1 Address Mapping Edit Screen	144
Chapter 11	
Firewalls	147
11.1 Firewall Overview	147
11.1.1 Stateful Inspection Firewalls	147
11.1.2 About the ZyXEL Device Firewall	147
11.1.3 Firewall Rule Direction	148
11.1.4 Firewall Rule Logic	149
11.1.4.1 Rule Checklist	149
11.1.4.2 Security Ramifications	149
11.1.5 Firewall Rule Services	149
11.1.6 DoS Thresholds	150
11.1.6.1 Threshold Values	150
11.1.6.2 Half-Open Sessions	150
11.1.6.3 TCP Maximum Incomplete and Blocking Time	151
11.2 Triangle Route	151
11.2.1 The "Triangle Route" Problem	152
11.2.2 Solving the "Triangle Route" Problem	152

11.3 Guidelines for Enhancing Security with Your Firewall	153
11.3.1 Security In General	153
11.4 General Firewall Screen	154
11.5 Firewall Rules Screen	155
11.5.1 Firewall Rule Edit Screen	157
11.5.2 Customized Services Screen	160
11.5.3 Customized Service Edit Screen	160
11.6 Anti-Probing Screen	161
11.7 Firewall Threshold Screen	162
Chapter 12	
Content Filter	165
12.1 Content Filtering Overview	165
12.2 Content Filtering Screens	165
12.2.1 Content Filter Screen	165
12.2.2 Content Filter Schedule Screen	167
Chapter 13	
Certificates	169
13.1 Certificates Overview	169
13.1.1 Advantages of Certificates	170
13.1.2 Self-signed Certificates	170
13.1.3 Certificate File Formats	170
13.2 My Certificates Screen	170
13.3 Import My Certificate Screen	172
13.4 Create My Certificate Screen	173
13.5 Edit My Certificates Screen	176
13.6 Trusted CAs Screen	179
13.7 Import Trusted CA Screen	181
13.8 Edit Trusted CA Screen	181
13.9 Trusted Remote Hosts Screen	184
13.10 Verifying a Trusted Remote Host's Certificate	186
13.11 Import Trusted Remote Host Screen	186
13.12 Edit Trusted Remote Host Screen	187
13.13 Directory Servers Screen	190
13.14 Edit Directory Server Screen	191
Chapter 14	
Static Route	193
14.1 Static Route Overview	193
14.2 IP Static Route Screen	193
14.2.1 Edit IP Static Route Screen	194

Chapter 15	
Bandwidth MGMT	197
15.1 Bandwidth Management Overview	197
15.1.1 Priority-based Scheduler	197
15.1.2 Bandwidth Management Priorities	197
15.1.3 Example: Unused and Unbudgeted Bandwidth	198
15.1.4 Reserving Bandwidth for Other Applications	198
15.1.5 Over Allotment of Bandwidth	199
15.2 Bandwidth Management Configuration Screen	199
15.3 Edit Bandwidth Management Rule Screen	202
15.4 Bandwidth Monitor	204
Chapter 16	
Remote MGMT	205
16.1 Remote Management Overview	205
16.1.1 Remote Management Limitations	205
16.1.2 Remote Management and NAT	206
16.1.3 System Timeout	206
16.1.4 SNMP	206
16.1.4.1 Supported MIBs	207
16.1.4.2 SNMP Traps	207
16.2 WWW Screen	208
16.3 Telnet Screen	210
16.4 FTP Screen	210
16.5 SNMP Screen	211
16.6 DNS Screen	213
16.7 Security Screen	213
16.8 SSH Screen	214
16.9 TR-069	215
Chapter 17	
UPnP	217
17.1 Introducing Universal Plug and Play	217
17.1.1 How do I know if I'm using UPnP?	217
17.1.2 NAT Traversal	217
17.1.3 Cautions with UPnP	217
17.2 UPnP and ZyXEL	218
17.3 UPnP Screen	218
17.4 Installing UPnP in Windows Example	219
17.5 Using UPnP in Windows XP Example	222

Chapter 18	
System	229
18.1 General Setup	229
18.1.1 General Setup and System Name	229
18.1.2 Dynamic DNS Overview	229
18.1.2.1 DYNDNS Wildcard	230
18.1.3 Resetting the Time	230
18.2 General System Screen	230
18.3 Dynamic DNS Screen	231
18.4 Time Setting Screen	233
Chapter 19	
Logs	237
19.1 Logs Overview	237
19.1.1 Alerts and Logs	237
19.2 View Log Screen	237
19.3 Log Settings Screen	238
Chapter 20	
Tools	241
20.1 Firmware Upgrade	241
20.2 Configuration Screen	242
20.3 Restart Screen	244
Chapter 21	
Introducing the SMT	247
21.1 Accessing the SMT	247
21.2 SMT Menu Items	248
21.3 Navigating the SMT Interface	251
Chapter 22	
General Setup	253
22.1 General Setup	253
22.2 Configure Dynamic DNS	254
22.3 Configure Dynamic DNS	255
Chapter 23	
WAN Setup	257
Chapter 24	
LAN Setup	259
24.1 LAN Port Filter Setup	259
24.2 TCP/IP and DHCP Ethernet Setup	260

24.3 IP Alias Setup	262
24.4 Wireless LAN Setup	263
24.5 WLAN MAC Address Filter	265
Chapter 25	
Internet Access Setup	267
Chapter 26	
Remote Node Setup	269
26.1 Remote Node Profile	269
26.2 Remote Node Network Layer Options	270
26.3 Remote Node Filter	272
26.4 Traffic Redirect Setup	273
Chapter 27	
Static Routing Setup	275
27.1 IP Static Route Setup	275
27.2 Edit IP Static Route	276
Chapter 28	
Dial-in User Setup	277
28.1 Dial-in User Setup	277
28.2 Edit Dial-in User	277
Chapter 29	
NAT Setup	279
29.1 Address Mapping Sets	279
29.2 Address Mapping Rules	279
29.3 Address Mapping Rule	281
29.4 NAT Server Setup	282
29.5 NAT Server Configuration	283
29.6 Trigger Port Setup	284
Chapter 30	
Filter Setup	287
30.1 Introduction to Filters	287
30.1.1 The Filter Structure of the ZyXEL Device	288
30.2 Configuring a Filter Set	289
30.2.1 Configuring a Filter Rule	292
30.2.2 Configuring a TCP/IP Filter Rule	292
30.2.3 Configuring a Generic Filter Rule	295
30.3 Example Filter	297
30.4 Filter Types and NAT	300
30.5 Firewall Versus Filters	300

30.6 Applying a Filter	300
30.6.1 Applying LAN Filters	300
30.6.2 Applying Remote Node Filters	301
30.7 Remote Node Profile	301
Chapter 31	
Firewall Setup	305
Chapter 32	
SNMP Configuration	307
Chapter 33	
System Security	309
33.1 Change Password	309
33.2 RADIUS Server	309
33.3 IEEE802.1x	310
Chapter 34	
System Maintenance 24.1 - 24.4	313
34.1 Status	313
34.2 Information	314
34.3 Change Console Port Speed	315
34.4 Syslog Logging	316
34.5 Call-Triggering Packet	317
34.6 Diagnostic	317
Chapter 35	
System Maintenance 24.5 - 24.7	319
35.1 Filename Conventions	319
35.2 Backup Configuration	320
35.2.1 Backup Configuration Using FTP	320
35.2.2 Using the FTP command from the DOS Prompt	321
35.2.3 Backup Configuration Using TFTP	322
35.2.4 Example: TFTP Command	323
35.2.5 Backup Via Console Port	323
35.3 Restore Configuration	324
35.3.1 Restore Using FTP	325
35.4 Uploading Firmware and Configuration Files	325
35.4.1 Firmware Upload	326
35.4.2 Configuration File Upload	326
35.4.3 Using the FTP command from the DOS Prompt Example	327
35.4.4 TFTP File Upload	328
35.4.5 Example: TFTP Command	328
35.4.6 Uploading Via Console Port	329

35.4.7 Uploading Firmware File Via Console Port	329
35.4.8 Example Xmodem Firmware Upload Using HyperTerminal	330
35.4.9 Uploading Configuration File Via Console Port	330
35.4.10 Example Xmodem Configuration Upload Using HyperTerminal	331
Chapter 36	
System Maintenance 24.8 - 24.11	333
36.1 Command Interpreter Mode	333
36.2 Budget Management	333
36.3 Call History	334
36.4 Time and Date Setting	335
36.5 Remote Management Control	337
Chapter 37	
IP Routing Policy Setup.....	339
37.1 Policy Route	339
37.2 Benefits	339
37.3 Routing Policy	339
37.4 IP Routing Policy Summary	340
37.5 IP Routing Policy Setup	341
37.6 IP Routing Policy Setup	342
37.7 IP Policy Routing Example	343
Chapter 38	
Schedule Setup	347
38.1 Schedule Set Overview	347
38.2 Schedule Setup	347
38.3 Schedule Set Setup	348
Chapter 39	
Troubleshooting	351
39.1 Problems Starting Up the ZyXEL Device	351
39.2 Problems with the LAN	351
39.3 Problems with the WAN	352
39.4 Problems Accessing the ZyXEL Device	353
39.4.1 Pop-up Windows, JavaScripts and Java Permissions	353
39.4.1.1 Internet Explorer Pop-up Blockers	353
39.4.1.2 JavaScripts	356
39.4.1.3 Java Permissions	358
39.4.2 ActiveX Controls in Internet Explorer	360
Appendix A	
Product Specifications	363

Appendix B	
Setting up Your Computer's IP Address.....	365
Windows 95/98/Me.....	365
Windows 2000/NT/XP	368
Macintosh OS X	373
Linux.....	375
Appendix C	
NetBIOS Filter Commands	379
Introduction	379
Display NetBIOS Filter Settings	379
NetBIOS Filter Configuration.....	380
Appendix D	
NAT.....	381
NAT Overview	381
NAT Definitions	381
What NAT Does	382
How NAT Works.....	382
NAT Application.....	383
NAT Mapping Types.....	383
NAT Types.....	384
SUA (Single User Account) Versus NAT	389
SUA Server	389
Appendix E	
Firewall Commands	391
Appendix F	
Log Descriptions.....	397
Log Commands.....	411
Log Command Example.....	412
Appendix G	
Boot Commands	413
Appendix H	
Internal SPTGEN	415
Internal SPTGEN Overview	415
The Configuration Text File Format.....	415
Internal SPTGEN FTP Download Example.....	416
Internal SPTGEN FTP Upload Example	417

Example Internal SPTGEN Menus.....	418
Appendix I	
Services	431
Index.....	435

List of Figures

Figure 1 Applications: Protected Internet Access	43
Figure 2 Applications: Management Server	43
Figure 3 LEDs	43
Figure 4 Connecting a POTS Splitter	45
Figure 5 Connecting a Microfilter	45
Figure 6 Login Screen	48
Figure 7 Login: Change Password Screen	48
Figure 8 Login: Replace Certificate Screen	49
Figure 9 Login: Select Mode Screen	49
Figure 10 Main Screen	50
Figure 11 Main Wizard Screen	55
Figure 12 Connection Wizard: Welcome	56
Figure 13 Connection Wizard: System Information	57
Figure 14 Connection Wizard: Wireless LAN	58
Figure 15 Connection Wizard: Wireless Security: None	59
Figure 16 Connection Wizard: Wireless Security: Basic Security Screen 1	60
Figure 17 Connection Wizard: Wireless Security: Basic Security Screen 2	61
Figure 18 Connection Wizard: Wireless Security: Auto	62
Figure 19 Connection Wizard: Wireless Security: Extend (WPA-PSK) Security Screen 1 ..	63
Figure 20 Connection Wizard: Wireless Security: Extend (WPA-PSK) Security Screen 2 ..	64
Figure 21 Connection Wizard: Wireless Security: Extend (WPA2-PSK) Security Screen 1 ..	65
Figure 22 Connection Wizard: Wireless Security: Extend (WPA2-PSK) Security Screen 2 ..	66
Figure 23 Connection Wizard: Internet Connection: Auto-Detection	67
Figure 24 Connection Wizard: ISP Parameters: Ethernet	68
Figure 25 Connection Wizard: ISP Parameters: PPPoE	69
Figure 26 Connection Wizard: IP Address Type	70
Figure 27 Connection Wizard: Static IP Address: Ethernet	71
Figure 28 Connection Wizard: ISP Parameters: PPPoE	72
Figure 29 Connection Wizard: MAC Address	73
Figure 30 Connection Wizard: Internet Configuration	74
Figure 31 Connection Wizard: OTIST: Start	75
Figure 32 Connection Wizard: Congratulations	75
Figure 33 Main Wizard Screen	78
Figure 34 BWM Wizard: Welcome	79
Figure 35 BWM Wizard: General Information	80
Figure 36 BWM Wizard: Services Setup	81
Figure 37 BWM Wizard: Priority Setup	83
Figure 38 BWM Wizard: Congratulations	84

Figure 39 Status	85
Figure 40 Status > BW MGMT Monitor	88
Figure 41 Status > DHCP Table	89
Figure 42 Status > Packet Statistics	89
Figure 43 Status > WLAN Station Status	90
Figure 44 Example of a Wireless Network	93
Figure 45 Network > Wireless LAN > General	97
Figure 46 Network > Wireless LAN > General > No Security	98
Figure 47 Network > Wireless LAN > General > Static WEP	98
Figure 48 Network > Wireless LAN > General > WPA-PSK	99
Figure 49 Network > Wireless LAN > General > WPA	100
Figure 50 Network > Wireless LAN > General > 802.1x + Dynamic WEP	102
Figure 51 Network > Wireless LAN > General > 802.1x + Static WEP	103
Figure 52 Network > Wireless LAN > General > 802.1x + No WEP	105
Figure 53 Network > Wireless LAN > General > WPA2-PSK	106
Figure 54 Network > Wireless LAN > General > WPA2	107
Figure 55 Network > Wireless LAN > OTIST	109
Figure 56 Example: Wireless Client OTIST Screen	110
Figure 57 OTIST: Settings	110
Figure 58 OTIST: In Progress on the ZyXEL Device	110
Figure 59 OTIST: In Progress on the Wireless Client	111
Figure 60 Start OTIST?	111
Figure 61 Network > Wireless LAN > MAC Filter	112
Figure 62 Network > Wireless LAN > Advanced	113
Figure 63 Network > WAN > Internet Connection > Ethernet	120
Figure 64 Network > WAN > Internet Connection > PPP over Ethernet	121
Figure 65 Network > WAN > Advanced	123
Figure 66 Network > WAN > Traffic Redirect	125
Figure 67 Example: IP Alias	129
Figure 68 Network > LAN > IP	129
Figure 69 Network > LAN > IP Alias	130
Figure 70 Network > LAN > Advanced	131
Figure 71 Network > DHCP Server > General	134
Figure 72 Network > DHCP Server > Static DHCP	135
Figure 73 Network > DHCP Server > Client List	136
Figure 74 Multiple Servers Behind NAT Example	137
Figure 75 Trigger Port Forwarding Process: Example	138
Figure 76 Network > NAT > General	139
Figure 77 Network > NAT > Port Forwarding	140
Figure 78 Network > NAT > Port Forwarding > Edit	141
Figure 79 Network > NAT > Trigger Port	142
Figure 80 Network > NAT > Address Mapping	143
Figure 81 Network > NAT > Address Mapping > Edit	144

Figure 82 Ideal Firewall Setup	151
Figure 83 “Triangle Route” Problem	152
Figure 84 IP Alias	153
Figure 85 Security > Firewall > General	154
Figure 86 Security > Firewall > Rules	156
Figure 87 Security > Firewall > Rules > Edit	158
Figure 88 Security > Firewall > Rules > Edit > Edit Customized Services	160
Figure 89 Security > Firewall > Rules > Edit > Edit Customized Services > Edit	161
Figure 90 Security > Firewall > Anti Probing	162
Figure 91 Security > Firewall > Threshold	163
Figure 92 Security > Content Filter > Filter	166
Figure 93 Security > Content Filter > Schedule	167
Figure 94 Security > Certificates > My Certificates	171
Figure 95 Security > Certificates > My Certificates > Import	173
Figure 96 Security > Certificates > My Certificates > Create	174
Figure 97 Security > Certificates > My Certificates > Create > In Progress	176
Figure 98 Security > Certificates > My Certificates > Create > Successful	176
Figure 99 Security > Certificates > My Certificates > Edit	177
Figure 100 Security > Certificates > Trusted CAs	180
Figure 101 Security > Certificates > Trusted CAs > Import	181
Figure 102 Security > Certificates > Trusted CAs > Edit	182
Figure 103 Security > Certificates > Trusted Remote Hosts	185
Figure 104 Certificate Details	186
Figure 105 Security > Certificates > Trusted Remote Host > Import	187
Figure 106 Security > Certificates > Trusted Remote Hosts > Edit	188
Figure 107 Security > Certificates > Directory Servers	190
Figure 108 Security > Certificates > Directory Servers > Edit	191
Figure 109 Example of Static Routing Topology	193
Figure 110 Management > Static Route > IP Static Route	194
Figure 111 Management > Static Route > IP Static Route > Edit	195
Figure 112 Management > Bandwidth MGMT > Configuration	200
Figure 113 Management > Bandwidth MGMT > Configuration > Edit	202
Figure 114 Management > Bandwidth MGMT > Monitor	204
Figure 115 SNMP Management Model	206
Figure 116 Management > Remote MGMT > WWW	209
Figure 117 Management > Remote MGMT > Telnet	210
Figure 118 Management > Remote MGMT > FTP	211
Figure 119 Management > Remote MGMT > SNMP	212
Figure 120 Management > Remote MGMT > DNS	213
Figure 121 Management > Remote MGMT > Security	213
Figure 122 Management > Remote MGMT > SSH	214
Figure 123 Enabling TR-069	215
Figure 124 Management > UPnP	218

Figure 125 Add/Remove Programs: Windows Setup: Communication	219
Figure 126 Add/Remove Programs: Windows Setup: Communication: Components	220
Figure 127 Network Connections	220
Figure 128 Windows Optional Networking Components Wizard	221
Figure 129 Networking Services	221
Figure 130 Network Connections	222
Figure 131 Internet Connection Properties	223
Figure 132 Internet Connection Properties: Advanced Settings	224
Figure 133 Internet Connection Properties: Advanced Settings: Add	224
Figure 134 System Tray Icon	225
Figure 135 Internet Connection Status	225
Figure 136 Network Connections	226
Figure 137 Network Connections: My Network Places	227
Figure 138 Network Connections: My Network Places: Properties: Example	227
Figure 139 Maintenance > System > General	230
Figure 140 Maintenance > System > Dynamic DNS	232
Figure 141 Maintenance > System > Time Setting	233
Figure 142 Maintenance > Logs > View Log	237
Figure 143 Maintenance > Logs > Log Settings	239
Figure 144 Maintenance > Tools > Firmware	241
Figure 145 Upload Firmware: In Progress	242
Figure 146 Upload Firmware: Network Temporarily Disconnected	242
Figure 147 Upload Firmware: Error	242
Figure 148 Maintenance > Tools > Configuration	243
Figure 149 Restore Configuration: Successful	244
Figure 150 Restore Configuration: Network Temporarily Disconnected	244
Figure 151 Restore Configuration: Error	244
Figure 152 Restart Screen	245
Figure 153 Login Screen	247
Figure 154 SMT Main Menu	248
Figure 155 Menu 1: General Setup	253
Figure 156 Menu 1.1: Configure Dynamic DNS	254
Figure 157 Menu 1.1.1: DDNS Edit Host	255
Figure 158 Menu 2: WAN Setup	257
Figure 159 Menu 3.1: LAN Port Filter Setup	259
Figure 160 Menu 3.2: TCP/IP and DHCP Ethernet Setup	260
Figure 161 Menu 3.2.1: IP Alias Setup	262
Figure 162 Menu 3.5: Wireless LAN Setup	264
Figure 163 Menu 3.5.1: WLAN MAC Address Filter	265
Figure 164 Menu 4: Internet Access Setup	267
Figure 165 Menu 11.1: Remote Node Profile	269
Figure 166 Menu 11.1.2: Remote Node Network Layer Options	271
Figure 167 Menu 11.1.4: Remote Node Filter	273

Figure 168 Menu 11.1.5: Traffic Redirect Setup	274
Figure 169 Menu 12: IP Static Route Setup	275
Figure 170 Menu 12.1: Edit IP Static Route	276
Figure 171 Menu 14: Dial-in User Setup	277
Figure 172 Menu 14.1: Edit Dial-in User	278
Figure 173 Menu 15.1: Address Mapping Sets	279
Figure 174 Menu 15.1.1: Address Mapping Rules	280
Figure 175 Menu 15.1.1.1: Address Mapping Rule	281
Figure 176 Menu 15.2: NAT Server Setup	283
Figure 177 Menu 15.2.1: NAT Server Configuration	284
Figure 178 Menu 15.3: Trigger Port Setup	285
Figure 179 Outgoing Packet Filtering Process	287
Figure 180 Filter Rule Process	289
Figure 181 Menu 21: Filter and Firewall Setup	290
Figure 182 Menu 21.1: Filter Set Configuration	290
Figure 183 Menu 21.1.1: Filter Rules Summary	291
Figure 184 Menu 21.1.1.1 TCP/IP Filter Rule.	293
Figure 185 Executing an IP Filter	295
Figure 186 Menu 21.1.1.1 Generic Filter Rule	296
Figure 187 Telnet Filter Example	298
Figure 188 Example Filter: Menu 21.1.3.1	298
Figure 189 Example Filter Rules Summary: Menu 21.1.3	299
Figure 190 Protocol and Device Filter Sets	300
Figure 191 Filtering LAN Traffic	301
Figure 192 Filtering Remote Node Traffic	301
Figure 193 Menu 11.1: Remote Node Profile	302
Figure 194 Menu 21.2: Firewall Setup	305
Figure 195 Menu 22: SNMP Configuration	307
Figure 196 Menu 23.1: System Security - Change Password	309
Figure 197 Menu 23.2: System Security - RADIUS Server	310
Figure 198 Menu 23.4: System Security - IEEE802.1x	311
Figure 199 Menu 24.1: System Maintenance - Status	313
Figure 200 Menu 24.2.1: System Maintenance - Information	315
Figure 201 Menu 24.2.2: System Maintenance - Change Console Port Speed	316
Figure 202 Menu 24.3.2: System Maintenance - Syslog Logging	316
Figure 203 Menu 24.3.4: Call-Triggering Packet (Example)	317
Figure 204 Menu 24.4: System Maintenance - Diagnostic	318
Figure 205 Menu 24.5: Backup Configuration	321
Figure 206 FTP Session Example	322
Figure 207 System Maintenance: Backup Configuration	324
Figure 208 System Maintenance: Starting Xmodem Download Screen	324
Figure 209 Backup Configuration Example	324
Figure 210 Successful Backup Confirmation Screen	324

Figure 211 Menu 24.6: Restore Configuration	325
Figure 212 Menu 24.7: System Maintenance - Upload Firmware	325
Figure 213 Menu 24.7.1: System Maintenance - Upload System Firmware	326
Figure 214 Menu 24.7.2: System Maintenance - Upload System Configuration File	327
Figure 215 FTP Session Example	328
Figure 216 Menu 24.7.1 as seen using the Console Port	329
Figure 217 Example Xmodem Upload	330
Figure 218 Menu 24.7.2 as seen using the Console Port	331
Figure 219 Example Xmodem Upload	331
Figure 220 Valid CI Commands	333
Figure 221 Menu 24.9.1: Budget Management	334
Figure 222 Menu 24.9.2: Call History	335
Figure 223 Menu 24.10: Time and Date Setting	336
Figure 224 Menu 24.11: Remote Management Control	338
Figure 225 Menu 25: IP Routing Policy Summary	340
Figure 226 Menu 25.1: IP Routing Policy Setup	341
Figure 227 Menu 25.1.1: IP Routing Policy Setup	343
Figure 228 IP Routing Policy Example	343
Figure 229 IP Routing Policy Example 1	344
Figure 230 IP Routing Policy Example 2	345
Figure 231 Menu 26: Schedule Setup	348
Figure 232 Menu 26.1: Schedule Set Setup	349
Figure 233 Pop-up Blocker	354
Figure 234 Internet Options	354
Figure 235 Internet Options	355
Figure 236 Pop-up Blocker Settings	356
Figure 237 Internet Options	357
Figure 238 Security Settings - Java Scripting	358
Figure 239 Security Settings - Java	359
Figure 240 Java (Sun)	360
Figure 241 Internet Options Security	361
Figure 242 Security Setting ActiveX Controls	362
Figure 243 Windows 95/98/Me: Network: Configuration	366
Figure 244 Windows 95/98/Me: TCP/IP Properties: IP Address	367
Figure 245 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	368
Figure 246 Windows XP: Start Menu	369
Figure 247 Windows XP: Control Panel	369
Figure 248 Windows XP: Control Panel: Network Connections: Properties	370
Figure 249 Windows XP: Local Area Connection Properties	370
Figure 250 Windows XP: Internet Protocol (TCP/IP) Properties	371
Figure 251 Windows XP: Advanced TCP/IP Properties	372
Figure 252 Windows XP: Internet Protocol (TCP/IP) Properties	373
Figure 253 Macintosh OS X: Apple Menu	374

Figure 254 Macintosh OS X: Network	374
Figure 255 Red Hat 9.0: KDE: Network Configuration: Devices	375
Figure 256 Red Hat 9.0: KDE: Ethernet Device: General	376
Figure 257 Red Hat 9.0: KDE: Network Configuration: DNS	376
Figure 258 Red Hat 9.0: KDE: Network Configuration: Activate	377
Figure 259 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	377
Figure 260 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	378
Figure 261 Red Hat 9.0: DNS Settings in resolv.conf	378
Figure 262 Red Hat 9.0: Restart Ethernet Card	378
Figure 263 Red Hat 9.0: Checking TCP/IP Properties	378
Figure 264 How NAT Works	382
Figure 265 NAT Application With IP Alias	383
Figure 266 Full Cone NAT Example	386
Figure 267 Restricted Cone NAT Example	387
Figure 268 Port Restricted Cone NAT Example	388
Figure 269 Symmetric NAT	389
Figure 270 Displaying Log Categories Example	411
Figure 271 Displaying Log Parameters Example	411
Figure 272 Option to Enter Debug Mode	413
Figure 273 Boot Module Commands	414
Figure 274 Configuration Text File Format: Column Descriptions	415
Figure 275 Invalid Parameter Entered: Command Line Example	416
Figure 276 Valid Parameter Entered: Command Line Example	416
Figure 277 Internal SPTGEN FTP Download Example	417
Figure 278 Internal SPTGEN FTP Upload Example	417

List of Tables

Table 1 LEDs	44
Table 2 Web Configurator: Navigation Panel and Icons	50
Table 3 Main Wizard Screen	55
Table 4 Connection Wizard: Welcome	56
Table 5 Connection Wizard: System Information	57
Table 6 Connection Wizard: Wireless LAN	58
Table 7 Connection Wizard: Wireless Security: None	59
Table 8 Connection Wizard: Wireless Security: Basic Security Screen 1	60
Table 9 Connection Wizard: Wireless Security: Basic Security Screen 2	61
Table 10 Connection Wizard: Wireless Security: Auto	62
Table 11 Connection Wizard: Wireless Security: Extend (WPA-PSK) Security Screen 1 ..	63
Table 12 Connection Wizard: Wireless Security: Extend (WPA-PSK) Security Screen 2 ..	64
Table 13 Connection Wizard: Wireless Security: Extend (WPA2-PSK) Security Screen 1	65
Table 14 Connection Wizard: Wireless Security: Extend (WPA2-PSK) Security Screen 2	66
Table 15 Connection Wizard: ISP Parameters: Ethernet	68
Table 16 Connection Wizard: ISP Parameters: PPPoE	69
Table 17 Connection Wizard: IP Address Type	70
Table 18 Connection Wizard: Static IP Address: Ethernet	71
Table 19 Connection Wizard: ISP Parameters: PPPoE	72
Table 20 Connection Wizard: MAC Address	73
Table 21 Connection Wizard: Internet Configuration	74
Table 22 Connection Wizard: Congratulations	75
Table 23 Main Wizard Screen	78
Table 24 BWM Wizard: Welcome	79
Table 25 BWM Wizard: General Information	80
Table 26 BWM Wizard: Services Setup	82
Table 27 BWM Wizard: Priority Setup	83
Table 28 BWM Wizard: Congratulations	84
Table 29 Status	86
Table 30 Status > DHCP Table	89
Table 31 Status > Packet Statistics	90
Table 32 Status > WLAN Station Status	91
Table 33 Types of Encryption for Each Type of User Authentication	95
Table 34 Network > Wireless LAN > General	97
Table 35 Network > Wireless LAN > General > No Security	98
Table 36 Network > Wireless LAN > General > Static WEP	99
Table 37 Network > Wireless LAN > General > WPA-PSK	99
Table 38 Network > Wireless LAN > General > WPA	101

Table 39 Network > Wireless LAN > General > 802.1x + Dynamic WEP	102
Table 40 Network > Wireless LAN > General > 802.1x + Static WEP	104
Table 41 Network > Wireless LAN > General > 802.1x + No WEP	105
Table 42 Network > Wireless LAN > General > WPA2-PSK	106
Table 43 Network > Wireless LAN > General > WPA2	108
Table 44 Network > Wireless LAN > OTIST	109
Table 45 Network > Wireless LAN > MAC Filter	112
Table 46 Network > Wireless LAN > Advanced	113
Table 47 Network > WAN > Internet Connection > Ethernet	120
Table 48 Network > WAN > Internet Connection > PPP over Ethernet	122
Table 49 Network > WAN > Advanced	123
Table 50 Network > WAN > Traffic Redirect	125
Table 51 Network > LAN > IP	129
Table 52 Network > LAN > IP Alias	130
Table 53 Network > LAN > Advanced	132
Table 54 Example: Assigning IP Addresses from a Pool	133
Table 55 Network > DHCP Server > General	134
Table 56 DHCP Setup	135
Table 57 Network > DHCP Server > Client List	136
Table 58 Network > NAT > General	139
Table 59 Network > NAT > Port Forwarding	140
Table 60 Network > NAT > Port Forwarding > Edit	141
Table 61 Network > NAT > Trigger Port	142
Table 62 Network > NAT > Address Mapping	144
Table 63 Network > NAT > Address Mapping > Edit	145
Table 64 Security > Firewall > General	155
Table 65 Security > Firewall > Rules	156
Table 66 Security > Firewall > Rules > Edit	159
Table 67 Security > Firewall > Rules > Edit > Edit Customized Services	160
Table 68 Security > Firewall > Rules > Edit > Edit Customized Services > Edit	161
Table 69 Security > Firewall > Anti Probing	162
Table 70 Security > Firewall > Threshold	163
Table 71 Security > Content Filter > Filter	166
Table 72 Security > Content Filter > Schedule	167
Table 73 Security > Certificates > My Certificates	171
Table 74 Security > Certificates > My Certificates > Import	173
Table 75 Security > Certificates > My Certificates > Create	174
Table 76 Security > Certificates > My Certificates > Edit	177
Table 77 Security > Certificates > Trusted CAs	180
Table 78 Security > Certificates > Trusted CAs > Import	181
Table 79 Security > Certificates > Trusted CAs > Edit	182
Table 80 Security > Certificates > Trusted Remote Hosts	185
Table 81 Security > Certificates > Trusted Remote Host > Import	187

Table 82 Security > Certificates > Trusted Remote Hosts > Edit	188
Table 83 Security > Certificates > Directory Servers	190
Table 84 Security > Certificates > Directory Servers > Edit	191
Table 85 Management > Static Route > IP Static Route	194
Table 86 Management > Static Route > IP Static Route > Edit	195
Table 87 Bandwidth Management Priorities	197
Table 88 Example: Priority-based Allotment of Unused and Unbudgeted Bandwidth	198
Table 89 Over Allotment of Bandwidth Example	199
Table 90 Management > Bandwidth MGMT > Configuration	201
Table 91 Management > Bandwidth MGMT > Configuration > Edit	203
Table 92 SNMPv1 Traps	207
Table 93 SNMPv2 Traps	208
Table 94 SNMP Interface Index to Physical Port Mapping	208
Table 95 Management > Remote MGMT > WWW	209
Table 96 Management > Remote MGMT > Telnet	210
Table 97 Management > Remote MGMT > FTP	211
Table 98 Management > Remote MGMT > SNMP	212
Table 99 Management > Remote MGMT > DNS	213
Table 100 Management > Remote MGMT > Security	214
Table 101 Management > Remote MGMT > SSH	215
Table 102 TR-069 Commands	216
Table 103 Configuring UPnP	218
Table 104 Maintenance > System > General	230
Table 105 Maintenance > System > Dynamic DNS	232
Table 106 Maintenance > System > Time Setting	234
Table 107 Maintenance > Logs > View Log	238
Table 108 Log Settings	239
Table 109 Maintenance > Tools > Firmware	241
Table 110 Maintenance > Tools > Configuration	243
Table 111 SMT Menus Overview	248
Table 112 Main Menu Commands	251
Table 113 Menu 1: General Setup	253
Table 114 Menu 1.1: Configure Dynamic DNS	254
Table 115 Menu 1.1.1: DDNS Edit Host	255
Table 116 Menu 2: WAN Setup	257
Table 117 Menu 3.1: LAN Port Filter Setup	259
Table 118 Menu 3.2: TCP/IP and DHCP Ethernet Setup	260
Table 119 Menu 3.2.1: IP Alias Setup	262
Table 120 Menu 3.5: Wireless LAN Setup	264
Table 121 Menu 3.5.1: WLAN MAC Address Filter	265
Table 122 Menu 4: Internet Access Setup	267
Table 123 Menu 11.1: Remote Node Profile	269
Table 124 Menu 11.1.2: Remote Node Network Layer Options	271

Table 125 Menu 11.1.4: Remote Node Filter	273
Table 126 Menu 11.1.5: Traffic Redirect Setup	274
Table 127 Menu 12: IP Static Route Setup	275
Table 128 Menu 12.1: Edit IP Static Route	276
Table 129 Menu 14: Dial-in User Setup	277
Table 130 Menu 14.1: Edit Dial-in User	278
Table 131 Menu 15.1: Address Mapping Sets	279
Table 132 Menu 15.1.1: Address Mapping Rules	280
Table 133 Menu 15.1.1.1: Address Mapping Rule	282
Table 134 Menu 15.2: NAT Server Setup	283
Table 135 Menu 15.2.1: NAT Server Configuration	284
Table 136 Menu 15.3: Trigger Port Setup	285
Table 137 Abbreviations Used in the Filter Rules Summary Menu	291
Table 138 Rule Abbreviations Used	291
Table 139 TCP/IP Filter Rule	293
Table 140 Generic Filter Rule Menu Fields	297
Table 141 Menu 11.1: Remote Node Profile	302
Table 142 Menu 22: SNMP Configuration	307
Table 143 Menu 23.1: System Security - Change Password	309
Table 144 Menu 23.2: System Security - RADIUS Server	310
Table 145 Menu 23.4: System Security - IEEE802.1x	311
Table 146 Menu 24.1: System Maintenance - Status	313
Table 147 Menu 24.2.1: System Maintenance - Information	315
Table 148 Menu 24.2.2: System Maintenance - Change Console Port Speed	316
Table 149 Menu 24.3.2: System Maintenance - Syslog Logging	316
Table 150 Menu 24.4: System Maintenance - Diagnostics	318
Table 151 Filename Conventions	320
Table 152 General Commands for Third Party FTP Clients	322
Table 153 General Commands for Third Party TFTP Clients	323
Table 154 Menu 24.9.1: Budget Management	334
Table 155 Menu 24.9.2: Call History	335
Table 156 Menu 24.10: Time and Date Setting	336
Table 157 Menu 24.11: Remote Management Control	338
Table 158 Menu 25: IP Routing Policy Summary	340
Table 159 Menu 25: IP Routing Policy Summary, Abbreviations	340
Table 160 Menu 25.1: IP Routing Policy Setup	341
Table 161 Menu 25.1.1: IP Routing Policy Setup	343
Table 162 Menu 26: Schedule Setup	348
Table 163 Menu 26.1: Schedule Set Setup	349
Table 164 Troubleshooting Starting Up Your ZyXEL Device	351
Table 165 Troubleshooting the LAN	351
Table 166 Troubleshooting the WAN	352
Table 167 Troubleshooting Accessing the ZyXEL Device	353

Table 168 Device Specifications	363
Table 169 NetBIOS Filter Default Settings	380
Table 170 NAT Definitions	381
Table 171 NAT Mapping Types	384
Table 172 NAT Types	385
Table 173 Firewall Commands	391
Table 174 System Maintenance Logs	397
Table 175 System Error Logs	398
Table 176 Access Control Logs	398
Table 177 TCP Reset Logs	399
Table 178 Packet Filter Logs	399
Table 179 ICMP Logs	400
Table 180 CDR Logs	400
Table 181 PPP Logs	400
Table 182 UPnP Logs	401
Table 183 Content Filtering Logs	401
Table 184 Attack Logs	402
Table 185 IPSec Logs	403
Table 186 IKE Logs	403
Table 187 PKI Logs	406
Table 188 Certificate Path Verification Failure Reason Codes	407
Table 189 802.1X Logs	408
Table 190 ACL Setting Notes	409
Table 191 ICMP Notes	409
Table 192 Syslog Logs	410
Table 193 RFC-2408 ISAKMP Payload Types	410
Table 194 Abbreviations Used in the Example Internal SPTGEN Screens Table	418
Table 195 Menu 1 General Setup	418
Table 196 Menu 3	418
Table 197 Menu 4 Internet Access Setup	422
Table 198 Menu 12	423
Table 199 Menu 15 SUA Server Setup	424
Table 200 Menu 21.1 Filter Set #1	425
Table 201 Menu 21.1 Filer Set #2	427
Table 202 Menu 23 System Menus	428
Table 203 Menu 24.11 Remote Management Control	429
Table 204 Examples of Services	431

Preface

Congratulations on your purchase of the P-870HW-I1 (“ZyXEL Device”) VDSL router with built-in IEEE 802.11g wireless capability. This ZyXEL Device also has a 4-port hub that allows you to connect up to 4 computers to the ZyXEL Device without purchasing a switch/hub.

About This User's Guide

This manual is designed to guide you through the configuration of your ZyXEL Device for its various applications. The web configurator parts of this guide contain background information on features configurable by web configurator.

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

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one of the predefined choices.
- 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-870HW-I1 may be referred to as the “ZyXEL Device” or the “device” in this User’s Guide.











Related Documentation

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

User Guide Feedback

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

Graphics Icons Key

<p>ZyXEL Device</p> 	<p>Computer</p> 	<p>Notebook computer</p> 
<p>Server</p> 	<p>DSLAM</p> 	<p>Firewall</p> 
<p>Telephone</p> 	<p>Switch</p> 	<p>Router</p> 
<p>Wireless Signal</p> 		

CHAPTER 1

Getting To Know Your ZyXEL Device

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

1.1 Introducing the ZyXEL Device

Your ZyXEL Device is a VDSL router that provides super high-speed Internet access through a telephone line. The ZyXEL Device supports high bandwidth applications such as video streaming, movies on demand, on-line gaming, video and Voice over IP (VoIP). The ZyXEL Device also has a built-in switch that allows you to connect up to four network devices and a built-in wireless network for additional devices.

Note: Actual speeds attained depend on the distance from your ISP, line quality, and so on.

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

1.2 Features

Triple-Play Service

The ZyXEL Device provides triple-play service for home users. Taking advantage of the benefits of SIP and UPnP, the ZyXEL Device offers security and convenience in the transfer of data, voice, and video.

High Speed Internet Access

The ZyXEL Device supports transmission speeds of up to 100 Mbps downstream and 50 Mbps upstream. Actual speeds attained depend on your ISP and how your ZyXEL Device is configured.

Quality of Service (QoS)

The ZyXEL Device with Quality of Service features to ensure high quality delivery of Triple Play Service using high-speed VDSL Internet access.

TR-069 Compliance

TR-069 is a protocol that defines how your ZyXEL Device can be managed via a management server such as ZyXEL's Vantage CNM Access. The management server can securely manage and update configuration changes in ZyXEL Devices.

PPPoE (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 VDSL. The PPPoE driver on the ZyXEL Device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers. The ZyXEL Device also includes PPPoE idle time-out (the PPPoE connection terminates after a period of no traffic that you configure) and PPPoE Dial-on-Demand (the PPPoE connection is brought up only when an Internet access request is made).

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). This can provide security and IP management. Powered by ZyNOS NAT technology, the ZyXEL Device supports NAT mapping, as well as most popular Internet multimedia applications, such as NetMeeting, CuSeeMe, IP TV, Quick Time, Real Player (RSP/RTSP), VoIP SIP ALG, and so on.

Firewall

The ZyXEL Device is 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 ZyXEL Device firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

Content Filtering

Content filtering allows you to block access to forbidden Internet web sites, schedule when the ZyXEL Device should perform the filtering and give trusted LAN IP addresses unfiltered Internet access.

Traffic Redirect

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

Media Bandwidth Management

ZyXEL's 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.

Universal Plug and Play (UPnP)

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

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. The ZyXEL Device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The ZyXEL Device can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

IP Alias

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

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.

1.2.1 Wireless Features

Wireless LAN

The ZyXEL Device supports the IEEE 802.11g standard, which is fully compatible with the IEEE 802.11b standard, meaning that you can have both IEEE 802.11b and IEEE 802.11g wireless clients in the same wireless network.

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

Wi-Fi Protected Access and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification standard. Key differences between WPA and WEP are user authentication and improved data encryption. WPA 2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

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

Antenna

The ZyXEL Device is equipped with one 2-dBi fixed antenna to provide clear radio signal between the wireless stations and the access points.

Output Power Management

Output power management is the ability to set the level of output power. There may be interference or difficulty with channel assignment when there is a high density of APs within a coverage area. In this case, you can lower the output power of each access point, thus enabling you to place access points closer together.

Wireless LAN MAC Address Filtering

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

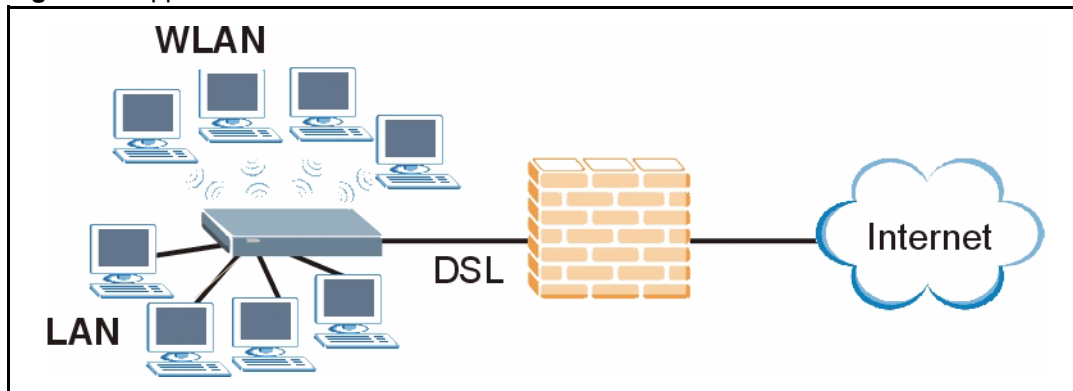
1.3 Application

The ZyXEL Device is the ideal high-speed Internet access solution. In addition, the ZyXEL Device allows wireless clients access to your network resources.

1.3.1 Protected Internet Access

The ZyXEL 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.

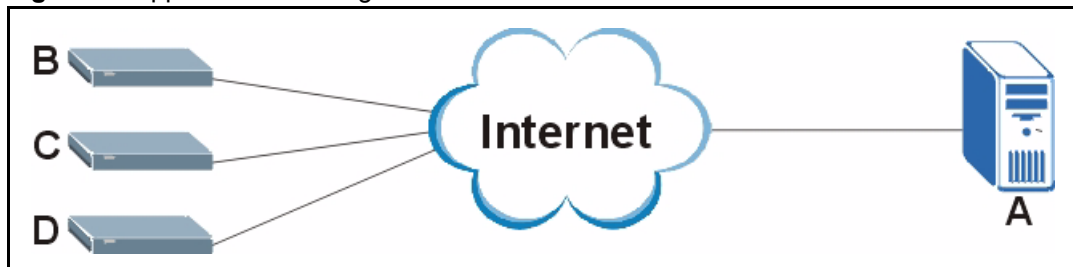
Figure 1 Applications: Protected Internet Access



1.3.2 Management Server

Your ZyXEL Device can be managed via a management server such as ZyXEL's Vantage CNM Access. The management server can securely manage and update configuration changes for you.

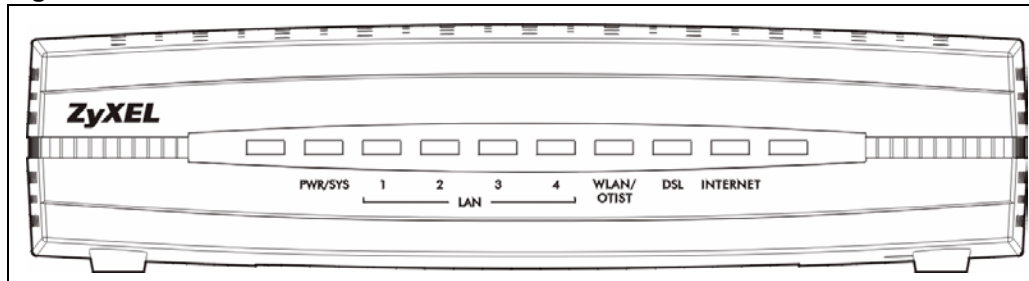
Figure 2 Applications: Management Server



1.4 LEDs

The following figure shows the LEDs.

Figure 3 LEDs



The following table describes the LEDs.

Table 1 LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting or performing diagnostics.
	Red	On	Power to the ZyXEL Device is too low, or there is a hardware error.
		Off	The system is not ready or has malfunctioned.
LAN (1-4)	Green	On	The ZyXEL Device has a good Ethernet connection.
		Blinking	The ZyXEL Device is sending or receiving data.
		Off	The LAN is not connected.
WLAN/ OTIST	Green	On	The ZyXEL Device is ready but is not sending or receiving data through the wireless LAN.
		Blinking	The ZyXEL Device is sending or receiving data through the wireless LAN.
	Amber	Blinking	The ZyXEL Device is using ZyXEL's One-Touch Intelligent Security Technology (OTIST).
		Off	The wireless LAN is not ready or has failed.
DSL	Green	On	The DSL line is up.
		Blinking	If the ZyXEL Device blinks slowly, it is trying to detect a carrier signal. If the ZyXEL Device blinks quickly, it is trying to train.
		Off	The DSL line is down.
INTERNET	Green	On	The Internet connection is up.
		Blinking	The ZyXEL Device is sending or receiving data.
	Red	On	The ZyXEL Device tried and failed to get an IP address.
		Off	The Internet connection is down.

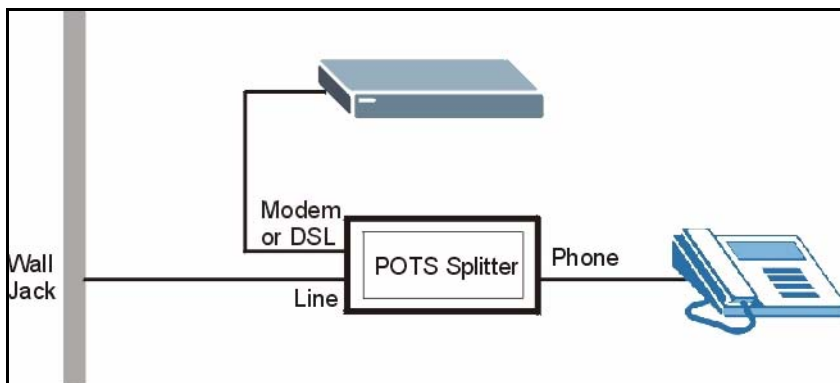
1.5 Splitters and Microfilters

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

1.5.1 Connecting a POTS Splitter

You can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and VDSL 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.

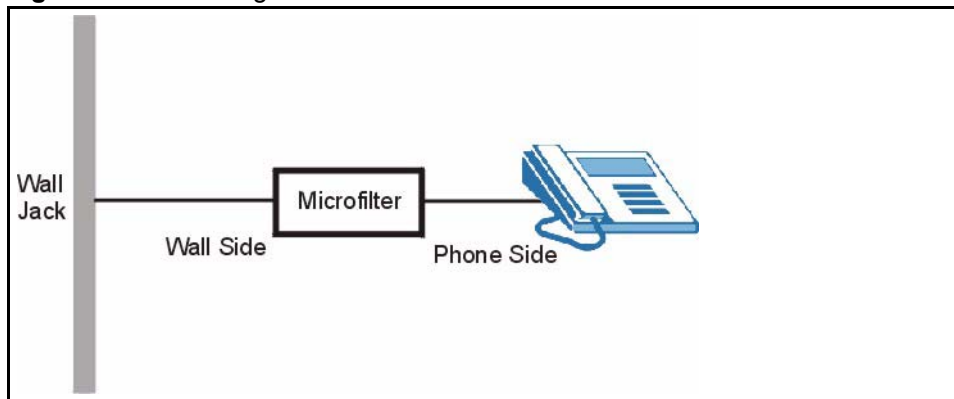
Figure 4 Connecting a POTS Splitter

- 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.

1.5.2 Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0-4 KHz, while VDSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that VDSL 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 5 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 ZyXEL Device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

See [Chapter 39 on page 351](#) if you need to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

Note: Even though you can connect to the ZyXEL Device wirelessly, it is recommended that you connect your computer to a **LAN** port for initial configuration.

- 1 Follow the directions in the Quick Start Guide to set up your ZyXEL Device and to connect your computer.
- 2 Launch your web browser, and go to <http://192.168.1.1>. The following screen appears.

Figure 6 Login Screen

The screenshot shows the login interface for the ZyXEL P-870HW-I1 router. At the top, the ZyXEL logo is displayed in white on a blue background. Below the logo, the model number "P-870HW-I1" is centered. The text "Welcome to your router Configuration Interface" is followed by the instruction "Enter your password and click 'Login'". A password field is shown with a key icon and the text "Password : ****", with a note below it stating "(max. 30 alphanumeric, printable characters and no spaces)". A yellow note icon is followed by the text "Note: Please turn on the Javascript and ActiveX control setting on Internet Explorer when operating system is Windows XP and service pack is SP2." At the bottom, there are two buttons: "Login" and "Reset".

- 3 The **Password** field may already contain the default password **1234**. If it does not, enter it. Click **Login**. The following screen appears.

Figure 7 Login: Change Password Screen

The screenshot shows the "Change Password" screen in the ZyXEL configuration interface. At the top, the ZyXEL logo is displayed in white on a blue background. Below the logo, the text "Please enter a new password" is centered. The main text reads: "Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess." Below this, it states: "The administrator password should must be between 1 - 30 characters." There are two password input fields: "New Password:" and "Retype to Confirm:". The "New Password:" field contains "****". At the bottom, there are two buttons: "Apply" and "Ignore".

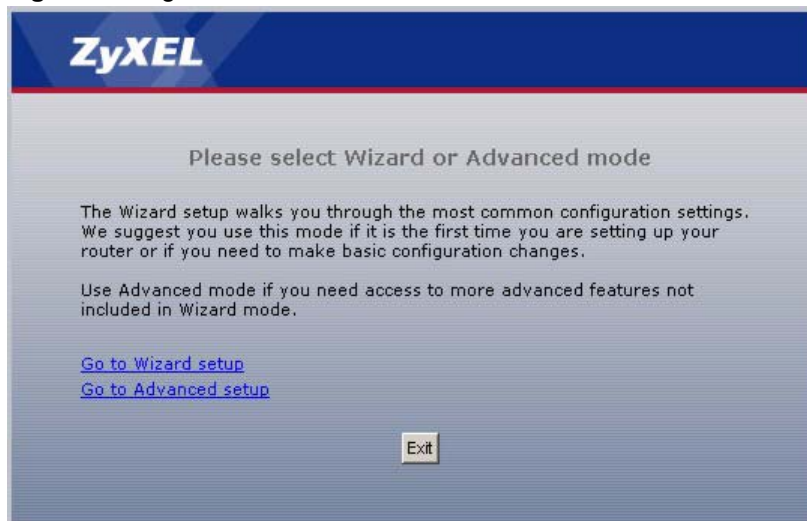
- 4 Follow the directions to change your password, or click **Cancel** to keep the default password. If you do not change your password, this screen appears the next time you log in.

Note: For security reasons, it is highly recommended that you change the password. You can change it here, or you can see [Chapter 18 on page 229](#).

Afterwards, the following screen appears.

Figure 8 Login: Replace Certificate Screen

- 5 Follow the directions in this screen. If you click **Ignore**, this screen appears the next time you log in. Afterwards, the following screen appears.

Figure 9 Login: Select Mode Screen

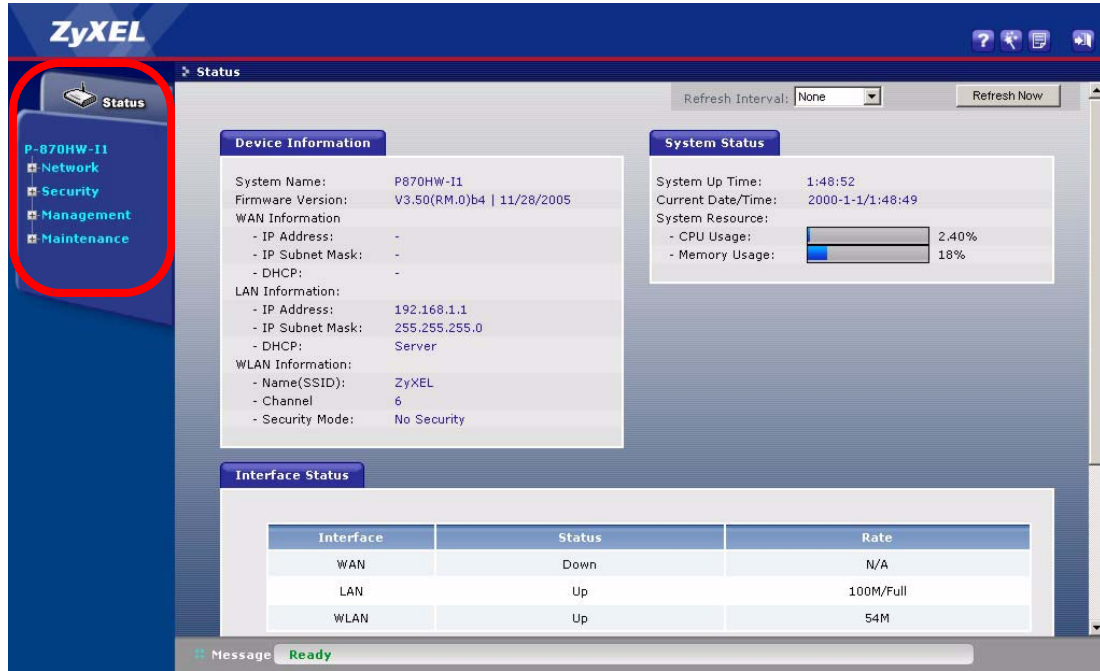
- 6 Select **Go to Wizard setup** to use the wizards. See [Chapter 3 on page 55](#) and [Chapter 4 on page 77](#). Select **Go to Advanced setup** to open the main screen. See [Section 2.3 on page 49](#).


Note: By default, the web configurator automatically times out in five minutes. Simply log back into the ZyXEL Device if this happens to you. You can change this setting; see [Chapter 18 on page 229](#).

2.3 Navigating the Web Configurator

The main screen is shown below. Your screen may be different, depending on the size of your browser window, resolution, and so on.

Figure 10 Main Screen



Note: Click the  icon (located in the upper right corner of most screens) to view embedded help.

The panel on the left side is the navigation panel. You can use this panel to open various screens in the web configurator.

The following table describes the icons in the upper right corner and the menu items in the navigation panel.

Table 2 Web Configurator: Navigation Panel and Icons




LINK/ICON	SUB-LINK	FUNCTION
Wizard 	INTERNET/WIRELESS SETUP	Use these screens to set up a basic wireless network and your Internet connection.
	BANDWIDTH MANAGEMENT SETUP	Use these screens to set the priority of various applications, in case there is not enough bandwidth for all of them.
About 		Click this icon to see the name of the device and copyright information.
Logout 		Click this icon to exit the web configurator.
Status		This screen shows the ZyXEL Device's general device, system and interface status information. You can also look at various statistics.
Network		

Table 2 Web Configurator: Navigation Panel and Icons (continued)

LINK/ICON	SUB-LINK	FUNCTION
Wireless LAN	General	Use this screen to configure basic wireless settings and wireless security.
	OTIST	Use this screen to activate ZyXEL's One-Touch Intelligent Security Technology (OTIST), which assigns the ZyXEL Device's wireless security settings to OTIST-compatible wireless devices.
	MAC Filter	Use this screen to block or allow other devices to access the ZyXEL Device.
	Advanced	Use this screen to set up roaming and other advanced wireless settings.
WAN	Internet Connection	Use this screen to configure ISP parameters, the WAN IP address, and the WAN MAC address.
	Advanced	Use this screen to set up DNS servers, RIP, multicasting, and other advanced settings.
	Traffic Redirect	Use this screen to set up a backup router, if you have one, in case the ZyXEL Device cannot access the Internet.
LAN	IP	Use this screen to set up the LAN IP address.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Advanced	Use this screen to set up RIP, multicasting, and other advanced settings.
DHCP Server	General	Use this screen to configure the ZyXEL Device's DHCP server, which assigns IP addresses and provides DNS server information to other computers on the LAN or WLAN.
	Static DHCP	Use this screen to assign the same IP address to a computer on the LAN or WLAN.
	Client List	Use this screen to look at the IP addresses of computers that have connected to the ZyXEL Device since the DHCP server was enabled.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the ZyXEL Device.
	Trigger Port	Use this screen to change your ZyXEL Device's port triggering settings.
	Address Mapping	Use this screen to configure network address translation mapping rules.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
Content Filter	Filter	Use this screen to block sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the ZyXEL Device to perform content filtering.

Table 2 Web Configurator: Navigation Panel and Icons (continued)

LINK/ICON	SUB-LINK	FUNCTION
Certificates	My Certificates	Use this screen to add, modify, or remove the ZyXEL Device's current certificates.
	Trusted CAs	Use this screen to add, modify, or remove certificates for other computers.
	Trusted Remote Hosts	Use this screen to add, modify, or remove certificates for other computers.
	Directory Servers	Use this screen to add, modify, or remove certificates for directory servers.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes.
Bandwidth MGMT	Configuration	Use this screen to set the priority of and to limit the amount of bandwidth used by various applications.
	Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or 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.
	Security	Use this screen to change your anti-probing settings.
	SSH	Use this screen to configure through which interface(s) and from which IP address(es) users can use SSH to access the ZyXEL Device.
UPnP	General	Use this screen to enable UPnP on the ZyXEL Device.
Maintenance		
System	General	This screen contains administrative and system-related information and also allows you to change your password.
	Dynamic DNS	Use this screen to set up dynamic DNS.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your ZyXEL Device's log settings.
Tools	Firmware	Use this screen to upload firmware to your ZyXEL Device.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your ZyXEL Device.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.

2.4 Resetting the ZyXEL Device

Reset the ZyXEL Device in the following situations:

- You forgot your password.
- You cannot access the device using the web configurator or SMT. Check **Troubleshooting** to make sure you cannot access the device anymore.

If you reset the ZyXEL Device, you lose all of the changes you have made. The ZyXEL Device re-loads its default settings, and the password resets to “1234”. You have to make all of your changes again.

Note: You will lose all of your changes when you push the **RESET** button.

To reset the ZyXEL Device,

- 1** Make sure the **PWR/SYS** light is on and not blinking.
- 2** Press and hold the **RESET** button until the **PWR/SYS** light begins to blink. (The **WLAN/OTIST** light might start blinking first. Wait until the **PWR/SYS** light starts blinking.) The default settings have been restored, and the ZyXEL Device begins to restart.

If the ZyXEL Device restarts automatically, wait for the ZyXEL Device to finish restarting, and log in to the web configurator. The password is **1234**. You have finished.

If the ZyXEL Device does not restart automatically, disconnect and reconnect the Prestige's power. Then, follow the directions above again.

CHAPTER 3

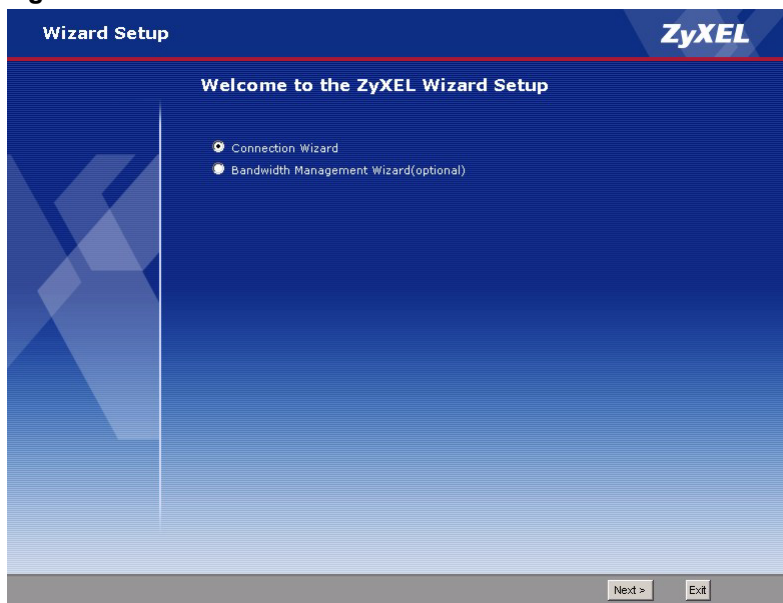
Connection Wizard

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

3.1 Main Wizard Screen

Use this screen to select which wizard you want to run.

Figure 11 Main Wizard Screen



The following table describes the labels in this screen.

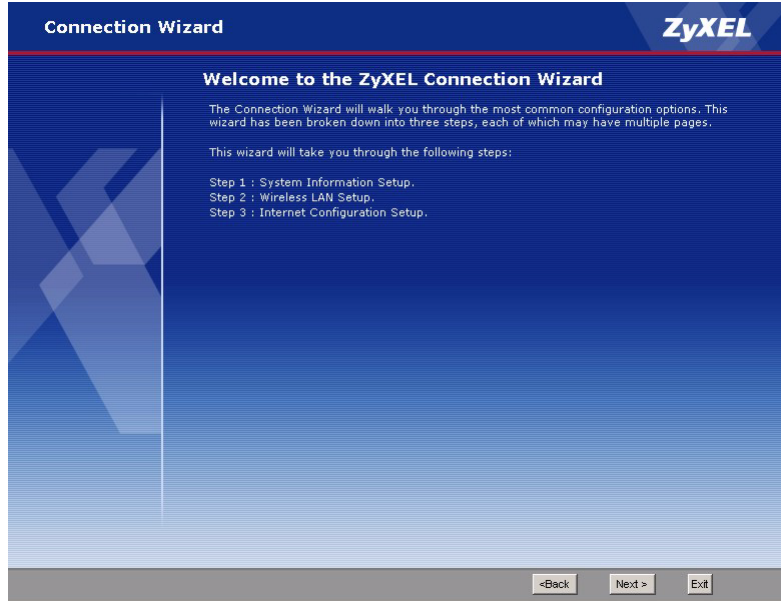
Table 3 Main Wizard Screen

LABEL	DESCRIPTION
Connection Wizard	Select this to set up a basic wireless network and your Internet connection.
Bandwidth Management Wizard	Select this to set the priority of various applications, in case there is not enough bandwidth for all of them.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.2 Welcome Screen

Use this screen to look at a preview of the **Connection Wizard**.

Figure 12 Connection Wizard: Welcome



The following table describes the labels in this screen.

Table 4 Connection Wizard: Welcome

LABEL	DESCRIPTION
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.3 System Information Screen

Use this screen to set up the system name and domain name for your ZyXEL Device.

Figure 13 Connection Wizard: System Information

Connection Wizard **ZyXEL**

STEP 1 | STEP 2 | STEP 3

System Information

System Name
Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.

System Name:

Domain Name
The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below. This field is normally left blank.

Domain Name:

<Back Next > Exit

The following table describes the labels in this screen.

Table 5 Connection Wizard: System Information

LABEL	DESCRIPTION
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.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.4 Wireless LAN Screen

Use this screen to set up the basic settings for your wireless network.

Figure 14 Connection Wizard: Wireless LAN

The following table describes the labels in this screen.

Table 6 Connection Wizard: Wireless LAN

LABEL	DESCRIPTION
Name(SSID)	The Service Set IDentity (SSID) is the name of the wireless network. Every wireless client in the same wireless network must use the same SSID. Enter this value as indicated.
Channel Selection	Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information. If there are other wireless networks in the area, select a channel at least five channels away from the other wireless networks.
Security	Select the strongest level that all the computers in your wireless network support. From weakest to strongest, the security levels are <ul style="list-style-type: none"> • None • Basic (WEP) • Auto or Extend (WPA-PSK). Select Auto if you want the ZyXEL Device to generate a pre-shared key for your wireless network. Select Extend if you want to set up a specific pre-shared key for your wireless network (for example, if your wireless network already uses a specific pre-shared key). • Extend (WPA2-PSK) If you want to use ZyXEL's One-Touch Intelligent Security Technology (OTIST), you can select any level except Extend(WPA2-PSK) , but it is simpler to select Auto .
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

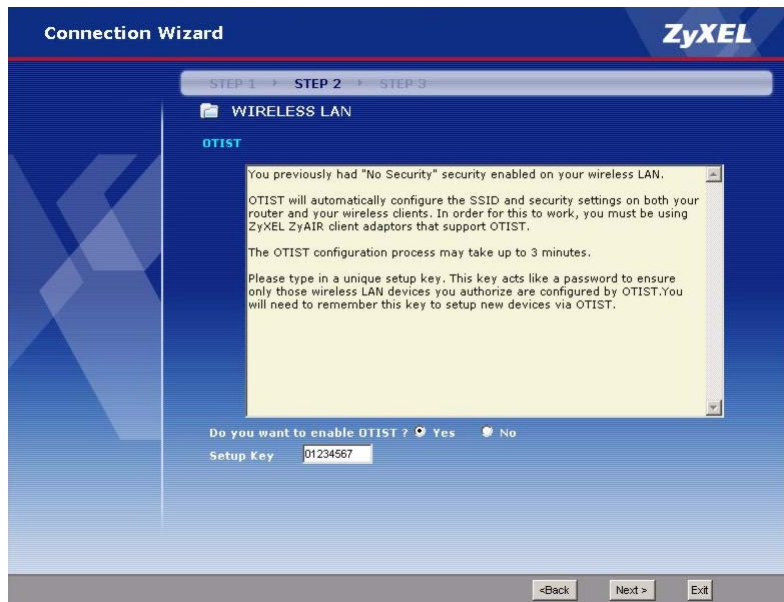
3.5 Wireless Security Screens

The next screens depend on which type of **Security** you select in the previous screen.

3.5.1 Wireless Security: None

Use this screen to enable OTIST for your wireless network.

Figure 15 Connection Wizard: Wireless Security: None



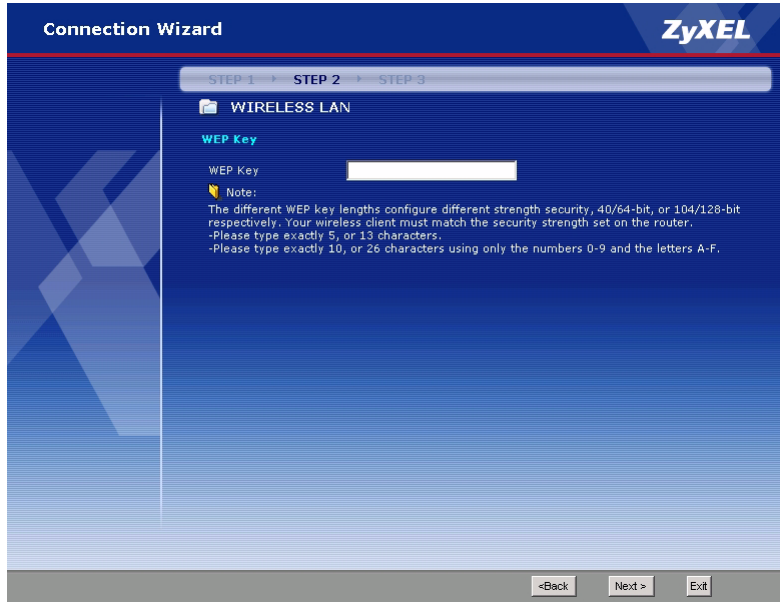
The following table describes the labels in this screen.

Table 7 Connection Wizard: Wireless Security: None

LABEL	DESCRIPTION
Do you want to enable OTIST?	Select Yes if you want to set up OTIST security. If you set up OTIST, your wireless network uses WPA-PSK security, not the security you selected and set up in the previous screen(s). See Section 6.5 on page 108 for more information about setting up OTIST.
Setup Key	Type a key (password) 8 ASCII characters long. Note: You must set up the same OTIST key on the wireless clients too.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.5.2 Wireless Security: Basic Security Screen 1

Use this screen to set up the WEP key(s) for your wireless network.

Figure 16 Connection Wizard: Wireless Security: Basic Security Screen 1

The following table describes the labels in this screen.

Table 8 Connection Wizard: Wireless Security: Basic Security Screen 1

LABEL	DESCRIPTION
WEP Key	Enter the key you want to use. You can enter the key using printable ASCII characters or hexadecimal (0-9, A-F, a-f) characters. The ZyXEL Device and the wireless stations must use the same WEP key. If you want to use a 64-bit WEP key, enter 5 printable ASCII characters or 10 hexadecimal characters. If you want to use a 128-bit WEP key, enter 13 printable ASCII characters or 26 hexadecimal characters. A 128-bit WEP key is more secure than a 64-bit WEP key.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.5.3 Wireless Security: Basic Security Screen 2

Use this screen to enable OTIST for your wireless network.

Figure 17 Connection Wizard: Wireless Security: Basic Security Screen 2



The following table describes the labels in this screen.

Table 9 Connection Wizard: Wireless Security: Basic Security Screen 2

LABEL	DESCRIPTION
Do you want to enable OTIST?	Select Yes if you want to set up OTIST security. If you set up OTIST, your wireless network uses WPA-PSK security, not the security you selected and set up in the previous screen(s). See Section 6.5 on page 108 for more information about setting up OTIST.
Setup Key	Type a key (password) 8 ASCII characters long. Note: You must set up the same OTIST key on the wireless clients too.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.5.4 Wireless Security: Auto

Use this screen to enable OTIST for your wireless network.

Figure 18 Connection Wizard: Wireless Security: Auto

The following table describes the labels in this screen.

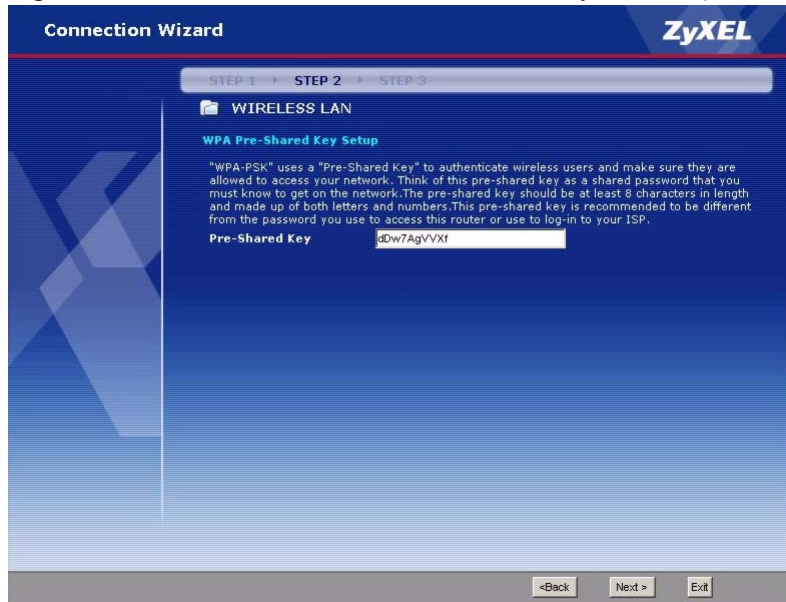
Table 10 Connection Wizard: Wireless Security: Auto

LABEL	DESCRIPTION
Do you want to enable OTIST?	Select Yes if you want to set up OTIST security. If you set up OTIST, your wireless network uses WPA-PSK security, not the security you selected and set up in the previous screen(s). See Section 6.5 on page 108 for more information about setting up OTIST.
Setup Key	Type a key (password) 8 ASCII characters long. Note: You must set up the same OTIST key on the wireless clients too.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.5.5 Wireless Security: Extend (WPA-PSK) Security Screen 1

Use this screen to set up the WPA pre-shared key for your wireless network.

Figure 19 Connection Wizard: Wireless Security: Extend (WPA-PSK) Security Screen 1



The following table describes the labels in this screen.

Table 11 Connection Wizard: Wireless Security: Extend (WPA-PSK) Security Screen 1

LABEL	DESCRIPTION
Pre-Shared Key	Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). The key is case-sensitive.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.5.6 Wireless Security: Extend (WPA-PSK) Security Screen 2

Use this screen to enable OTIST for your wireless network.

Figure 20 Connection Wizard: Wireless Security: Extend (WPA-PSK) Security Screen 2

The following table describes the labels in this screen.

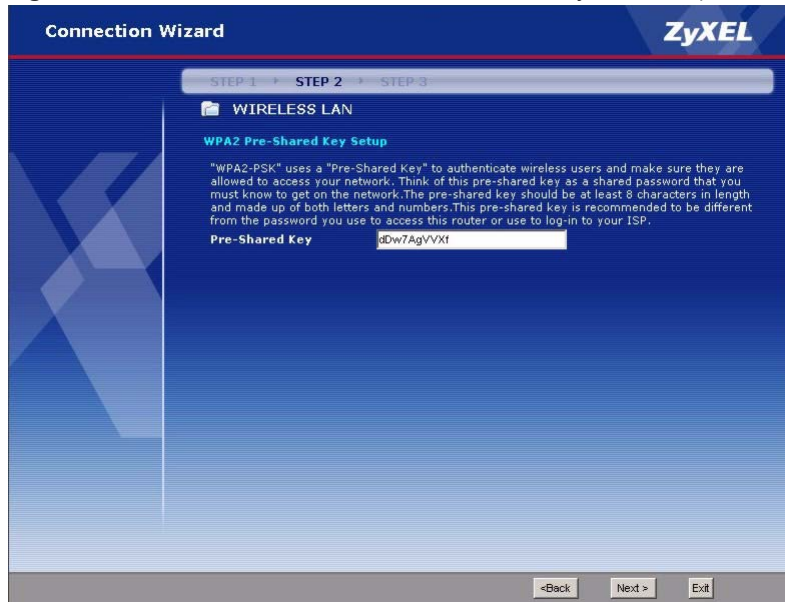
Table 12 Connection Wizard: Wireless Security: Extend (WPA-PSK) Security Screen 2

LABEL	DESCRIPTION
Do you want to enable OTIST?	Select Yes if you want to set up OTIST security. If you set up OTIST, your wireless network uses WPA-PSK security, not the security you selected and set up in the previous screen(s). See Section 6.5 on page 108 for more information about setting up OTIST.
Setup Key	Type a key (password) 8 ASCII characters long. Note: You must set up the same OTIST key on the wireless clients too.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.5.7 Wireless Security: Extend (WPA2-PSK) Security Screen 1

Use this screen to set up the WPA2 pre-shared key for your wireless network.

Figure 21 Connection Wizard: Wireless Security: Extend (WPA2-PSK) Security Screen 1



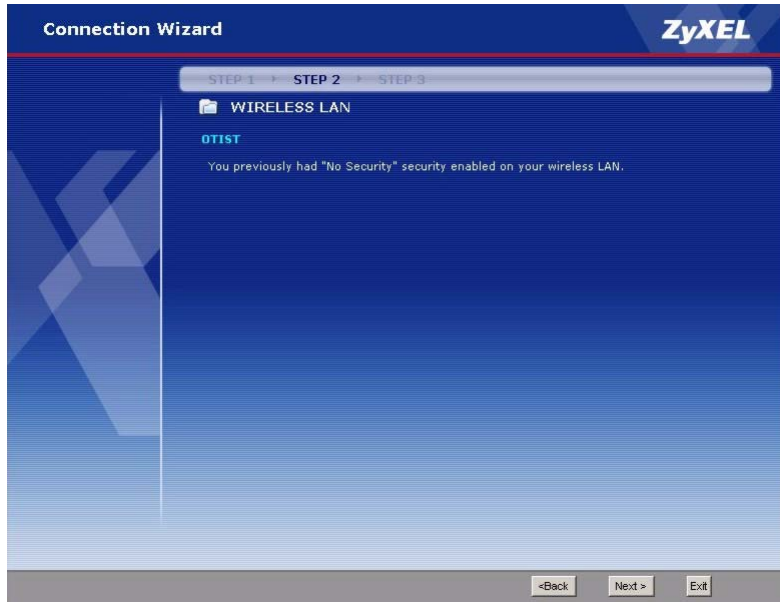
The following table describes the labels in this screen.

Table 13 Connection Wizard: Wireless Security: Extend (WPA2-PSK) Security Screen 1

LABEL	DESCRIPTION
Pre-Shared Key	Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). The key is case-sensitive.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.5.8 Wireless Security: Extend (WPA2-PSK) Security Screen 2

Figure 22 Connection Wizard: Wireless Security: Extend (WPA2-PSK) Security Screen 2



The following table describes the labels in this screen.

Table 14 Connection Wizard: Wireless Security: Extend (WPA2-PSK) Security Screen 2

LABEL	DESCRIPTION
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.6 Auto-Detection Screen

Wait while your ZyXEL Device tries to detect your Internet connection.

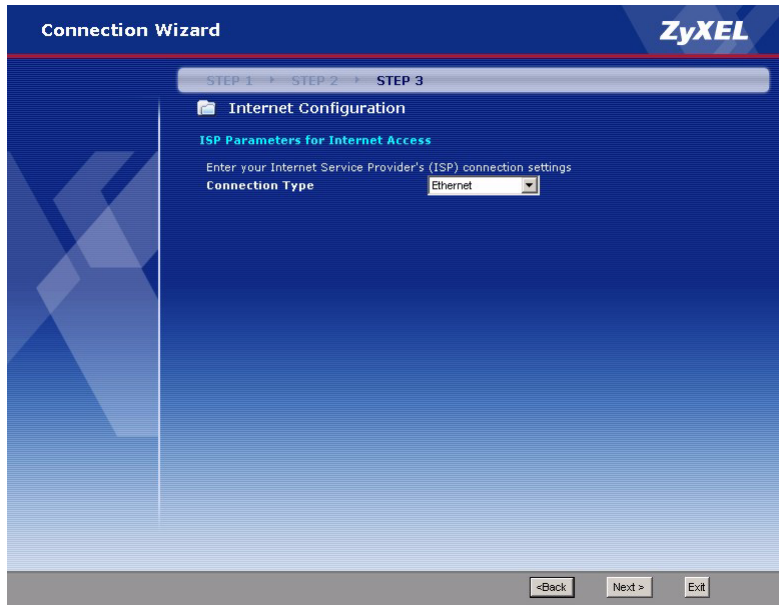
Figure 23 Connection Wizard: Internet Connection: Auto-Detection

3.7 ISP Parameters Screen

Use these screens to set up your Internet connection. The screen depends on which type of **Connection Type** your Internet connection uses. If your ISP provided you a user name and password, select **PPP over Ethernet**. Otherwise, select **Ethernet**.

3.7.1 ISP Parameters: Ethernet Screen

Use this screen to set up an Ethernet connection to the Internet.

Figure 24 Connection Wizard: ISP Parameters: Ethernet

The following table describes the labels in this screen.

Table 15 Connection Wizard: ISP Parameters: Ethernet

LABEL	DESCRIPTION
Connection Type	Select Ethernet .
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.7.2 ISP Parameters: PPPoE Screen

Use this screen to set up a PPPoE connection to the Internet.

Figure 25 Connection Wizard: ISP Parameters: PPPoE

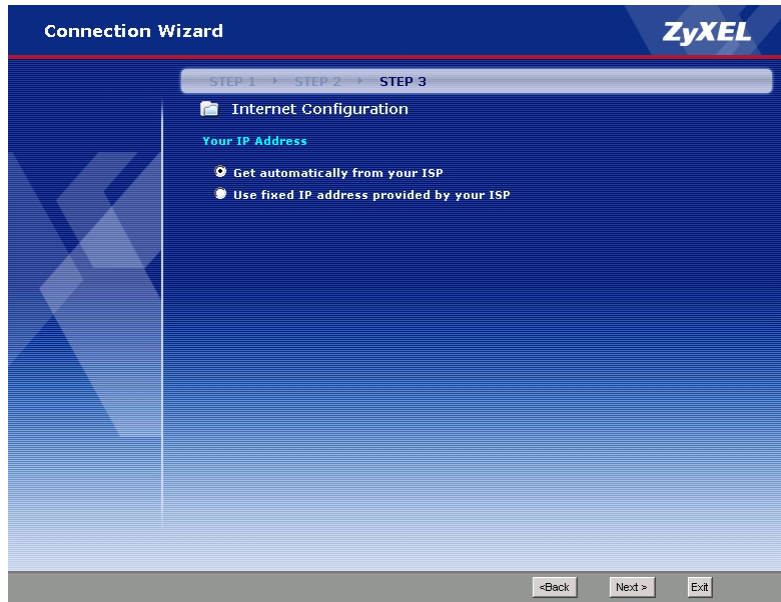
The following table describes the labels in this screen.

Table 16 Connection Wizard: ISP Parameters: PPPoE

LABEL	DESCRIPTION
Connection Type	Select PPP over Ethernet .
Service Name	Enter the service name provided by your ISP. Leave this field blank if your ISP did not provide one.
User Name	Enter the user name provided by your ISP.
Password	Enter the password provided by your ISP.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.8 IP Address Type Screen

Use this screen to specify what type of IP address your ISP provides.

Figure 26 Connection Wizard: IP Address Type

The following table describes the labels in this screen.

Table 17 Connection Wizard: IP Address Type

LABEL	DESCRIPTION
Get automatically from ISP	Select this if your ISP did not give you a fixed (static) IP address.
Use fixed IP address provided by your ISP	Select this if your ISP gave you a fixed (static) IP address.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.9 Static IP Address Settings Screen

Use these screens to set up a static IP address. The screen depends on which type of **Connection Type** your Internet connection uses.

3.9.1 Static IP Address Settings: Ethernet Screen

Use this screen to set up a static IP address for an Ethernet connection to the Internet.

Figure 27 Connection Wizard: Static IP Address: Ethernet

The following table describes the labels in this screen.

Table 18 Connection Wizard: Static IP Address: Ethernet

LABEL	DESCRIPTION
My WAN IP Address	Enter the fixed (static) IP address provided by your ISP.
My WAN IP Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the IP address of the gateway provided by your ISP.
DNS Servers	DNS (Domain Name System) manages the relationships between domain names and IP addresses. For example, the IP address of www.zyxel.com is 204.217.0.2. Without a DNS server, you must know the IP address of the computer you want to access before you access it.
First DNS Server Second DNS Server Third DNS Server	Enter the IP address of each DNS server provided by your ISP. Use the default value, if your ISP did not provide IP addresses for three DNS servers.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.9.2 ISP Parameters: PPPoE Screen

Use this screen to set up a PPPoE connection to the Internet.

Figure 28 Connection Wizard: ISP Parameters: PPPoE

The screenshot shows the 'Connection Wizard' interface for ZyXEL. It is currently on 'STEP 3' of the 'Internet Configuration' process. Under 'WAN IP Address Assignment', the 'My WAN IP Address' is set to 0.0.0.0. Under 'DNS Server Address Assignment', the 'First DNS Server', 'Second DNS Server', and 'Third DNS Server' are all set to 0.0.0.0. At the bottom, there are buttons for '<Back', 'Next >', and 'Exit'.

The following table describes the labels in this screen.

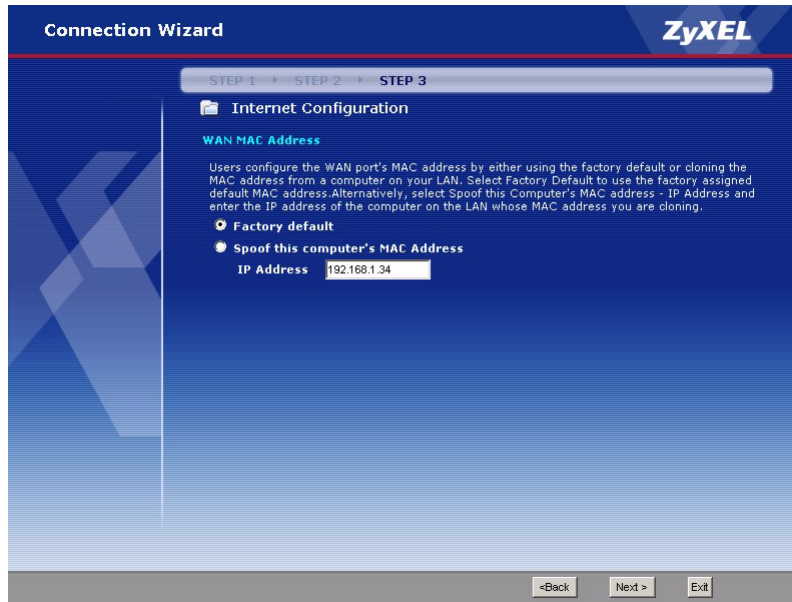
Table 19 Connection Wizard: ISP Parameters: PPPoE

LABEL	DESCRIPTION
My WAN IP Address	Enter the fixed (static) IP address provided by your ISP.
DNS Servers	DNS (Domain Name System) manages the relationships between domain names and IP addresses. For example, the IP address of www.zyxel.com is 204.217.0.2. Without a DNS server, you must know the IP address of the computer you want to access before you access it.
First DNS Server Second DNS Server Third DNS Server	Enter the IP address of each DNS server provided by your ISP. Use the default value, if your ISP did not provide IP addresses for three DNS servers.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.10 MAC Address Screen

Use this screen to specify which MAC address the ZyXEL Device should use.

Figure 29 Connection Wizard: MAC Address



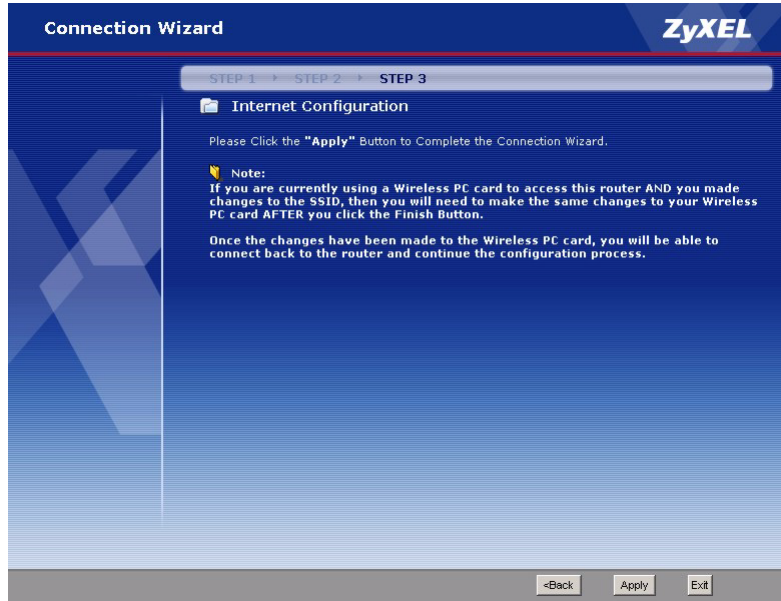
The following table describes the labels in this screen.

Table 20 Connection Wizard: MAC Address

LABEL	DESCRIPTION
Factory default	Select this, unless you have spoofed (cloned) your computer's MAC address before.
Spoof this computer's MAC Address	Select this if you want the ZyXEL Device to use the MAC address of another computer, instead of its default MAC address. You might try this if you lose your Internet connection because some ISPs check the MAC address of the device connected to the Internet.
IP Address	If you select Spoof this computer's MAC Address , enter the IP address of the computer whose MAC address you want the ZyXEL Device to use. This is usually a computer on the LAN.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.11 Internet Configuration Screen

Figure 30 Connection Wizard: Internet Configuration



The following table describes the labels in this screen.

Table 21 Connection Wizard: Internet Configuration

LABEL	DESCRIPTION
Back	Click this to return to the previous screen.
Apply	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

3.12 Auto-Detection Screen

If you enabled OTIST, wait while your ZyXEL Device starts OTIST. You have to start OTIST on the wireless clients within three minutes of seeing this screen.

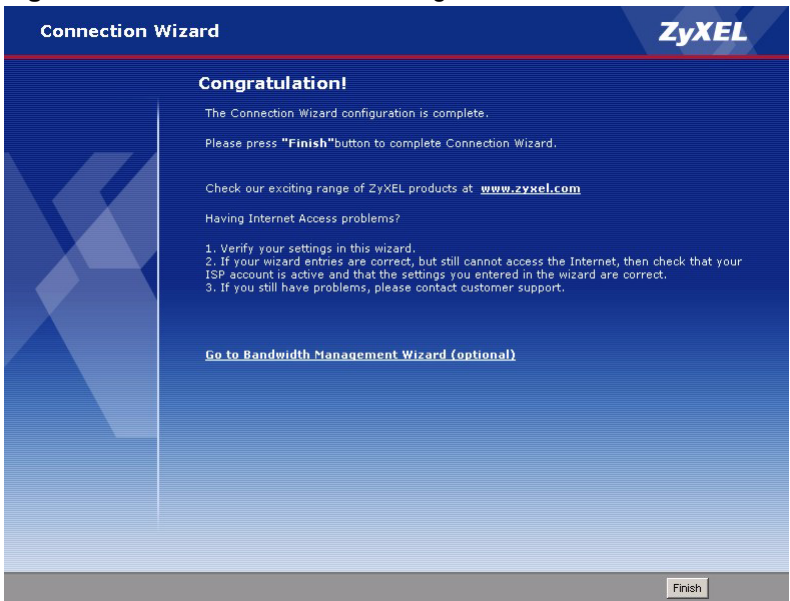
Figure 31 Connection Wizard: OTIST: Start



3.13 Congratulations Screen

Use this screen to finish the **Connection Wizard**.

Figure 32 Connection Wizard: Congratulations



The following table describes the labels in this screen.

Table 22 Connection Wizard: Congratulations

LABEL	DESCRIPTION
Finish	Click this to close the wizard.

CHAPTER 4

Bandwidth Management Wizard

This chapter provides information on the Wizard Setup screens for bandwidth management.

Bandwidth management is only useful when the ZyXEL Device is trying to send more traffic out through than the WAN port than the WAN port can support. In this case, bandwidth management allows you to control the amount of traffic going out through the WAN port and which applications can use this traffic. You specify which applications can use this traffic by assigning each one a priority and how much bandwidth it is allocated.

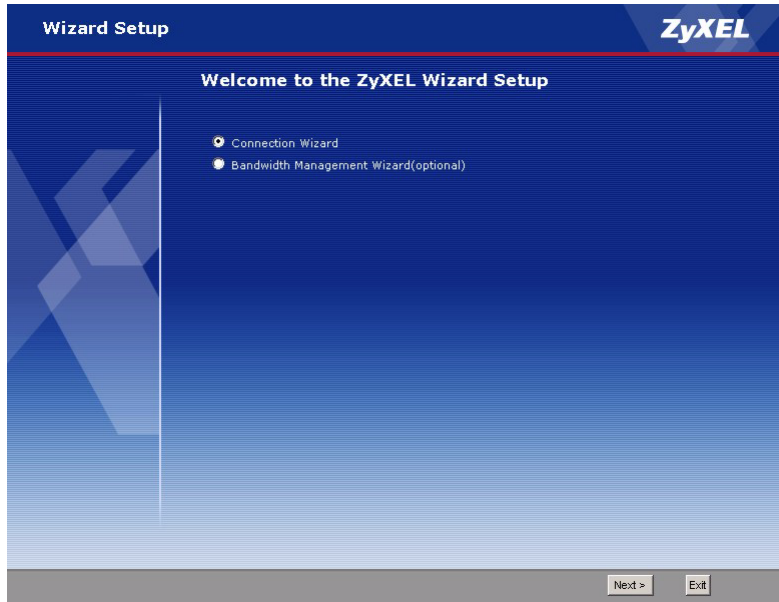
- High-priority applications get to use their allocation first.
- If there is more bandwidth left, medium-priority applications get to use their allocation.
- If there is still more bandwidth left, low-priority applications get to use their allocation.
- If there is still more bandwidth, all applications, including those above and other types of applications, share it.

Some applications, such as VoIP and online gaming, need to have enough bandwidth to provide acceptable quality. These applications usually have high priority. Other applications, such as web surfing and e-mail, might run more slowly if there is not a lot of bandwidth, but the quality is still adequate. These applications have medium or low priority. There are still other applications, such as some large file transfers, that are less urgent than the first two kinds of applications. You do not usually allocate any bandwidth to these applications because these applications only get bandwidth when other applications are not using it.

This wizard helps you set the priority of some pre-defined applications. Use **Maintenance > Bandwidth MGMT** to change the amount of bandwidth allocated to each one or to set up priorities and allocations for other types of applications.

4.1 Main Wizard Screen

Use this screen to select which wizard you want to run.

Figure 33 Main Wizard Screen

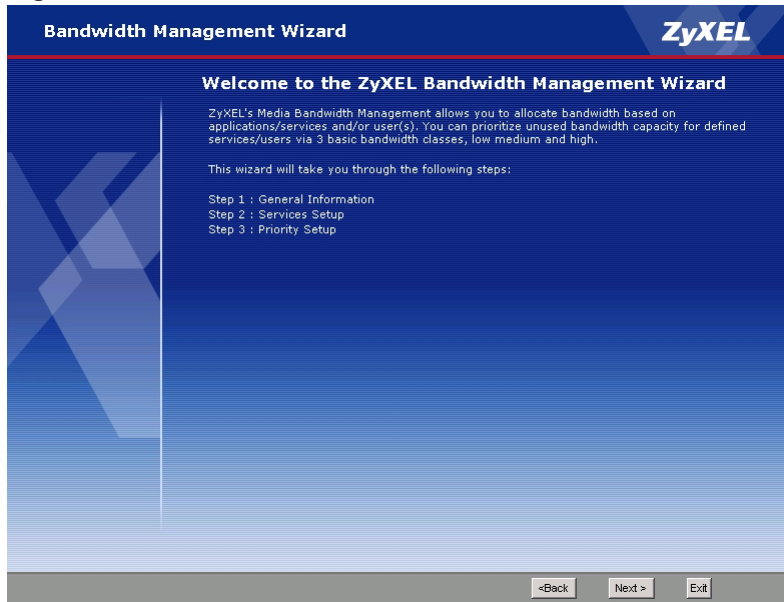
The following table describes the labels in this screen.

Table 23 Main Wizard Screen

LABEL	DESCRIPTION
Connection Wizard	Select this to set up a basic wireless network and your Internet connection.
Bandwidth Management Wizard	Select this to set the priority of various applications, in case there is not enough bandwidth for all of them.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

4.2 Welcome Screen

Use this screen to look at a preview of the **Bandwidth Management Wizard**.

Figure 34 BWM Wizard: Welcome

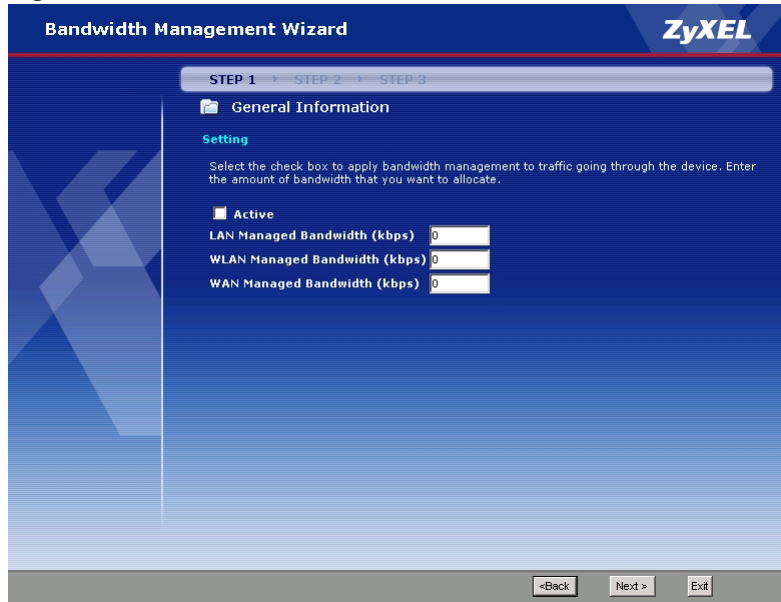
The following table describes the labels in this screen.

Table 24 BWM Wizard: Welcome

LABEL	DESCRIPTION
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

4.3 General Information Screen

Use this screen to activate bandwidth management and to set the amount of bandwidth you want to allocate for each interface on the ZyXEL Device.

Figure 35 BWM Wizard: General Information

The following table describes the labels in this screen.

Table 25 BWM Wizard: General Information

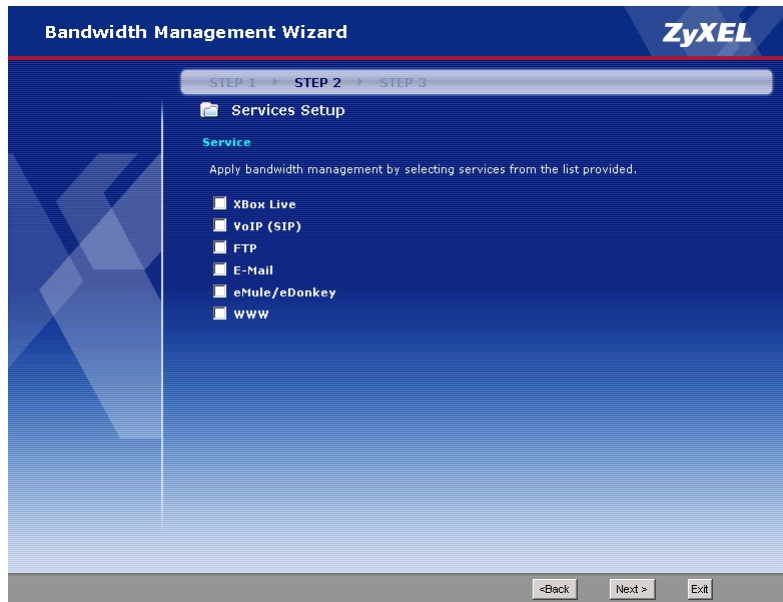
LABEL	DESCRIPTION
Active	Select this to enable bandwidth management.
LAN Managed Bandwidth	<p>Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.</p> <p>It is recommended to set this speed to match what the LAN port's connection can handle. For example, set it to 100000 kbps if your Ethernet network has a maximum speed of 100000 kbps.</p> <p>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.</p> <p>You can also set this number lower than the interface's actual transmission speed. However, this will cause the ZyXEL Device to not use some of the interface's available bandwidth.</p>
WLAN Managed Bandwidth	<p>Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.</p> <p>It is recommended to set this speed to match the maximum speed of the wireless network. In most cases, set it to 54000 kbps, unless your wireless network cannot handle this speed.</p> <p>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.</p> <p>You can also set this number lower than the interface's actual transmission speed. However, this will cause the ZyXEL Device to not use some of the interface's available bandwidth.</p>

Table 25 BWM Wizard: General Information (continued)

LABEL	DESCRIPTION
WAN Managed Bandwidth	<p>Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.</p> <p>It is recommended to set this speed to match what the WAN port's connection can handle. For example, set it to 40000 kbps if your broadband modem or router has a maximum speed of 40000 kbps.</p> <p>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.</p> <p>You can also set this number lower than the interface's actual transmission speed. However, this will cause the ZyXEL Device to not use some of the interface's available bandwidth.</p>
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

4.4 Services Setup Screen

Use this screen to select the applications to which you want to allocate bandwidth. You can use the applications you do not select, as well as ones that do not appear on this list, but they have lower priority.

Figure 36 BWM Wizard: Services Setup

The following table describes the labels in this screen.

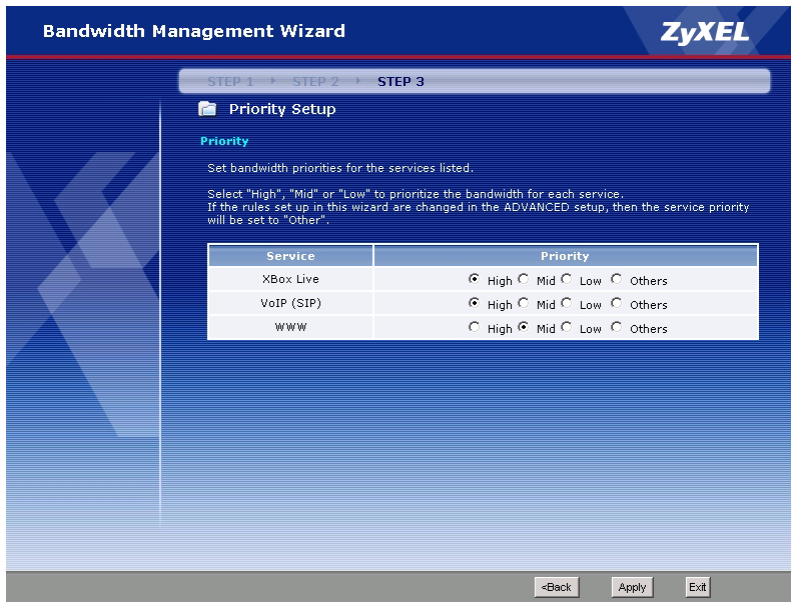
Table 26 BWM Wizard: Services Setup

LABEL	DESCRIPTION
Xbox Live	This is Microsoft's online gaming service that lets you play multiplayer Xbox games on the Internet via broadband technology. Xbox Live uses port 3074.
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80
eMule/eDonkey	These programs use advanced file sharing applications relying on central servers to search for files. They use default port 4662.
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.
Back	Click this to return to the previous screen.
Next	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

4.5 Priority Setup Screen

Use this screen to set the priority of the applications you selected in the previous screen.

Figure 37 BWM Wizard: Priority Setup



The following table describes the labels in this screen.

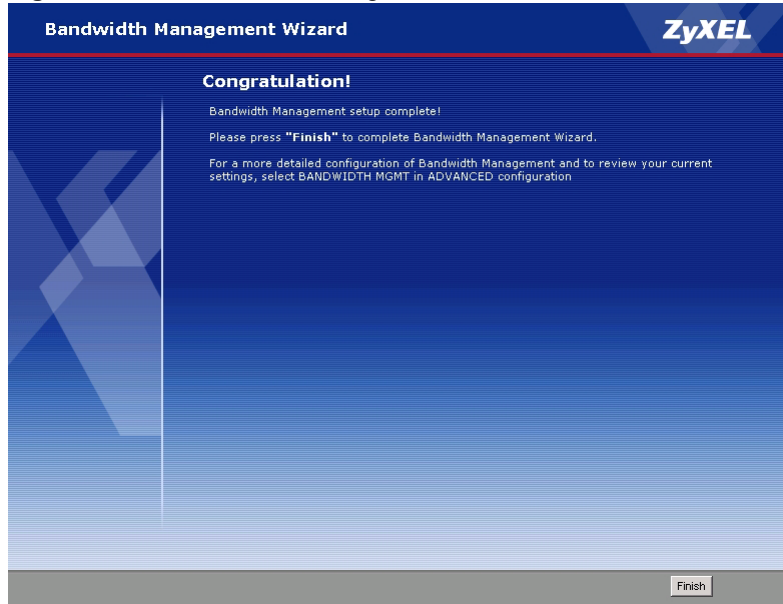
Table 27 BWM Wizard: Priority Setup

LABEL	DESCRIPTION
Service	This field displays the applications you selected in the previous screen.
Priority	Select the priority of each application. Other applications have lower priority than all the applications in this screen, including ones to which you assign Low priority.
Back	Click this to return to the previous screen.
Apply	Click this to save your changes on this screen and to proceed to the next screen.
Exit	Click this to close the wizard without saving the changes on this screen.

4.6 Congratulations Screen

Use this screen to finish the **Bandwidth Management Wizard**.

Figure 38 BWM Wizard: Congratulations



The following table describes the labels in this screen.

Table 28 BWM Wizard: Congratulations

LABEL	DESCRIPTION
Finish	Click this to close the wizard.

CHAPTER 5

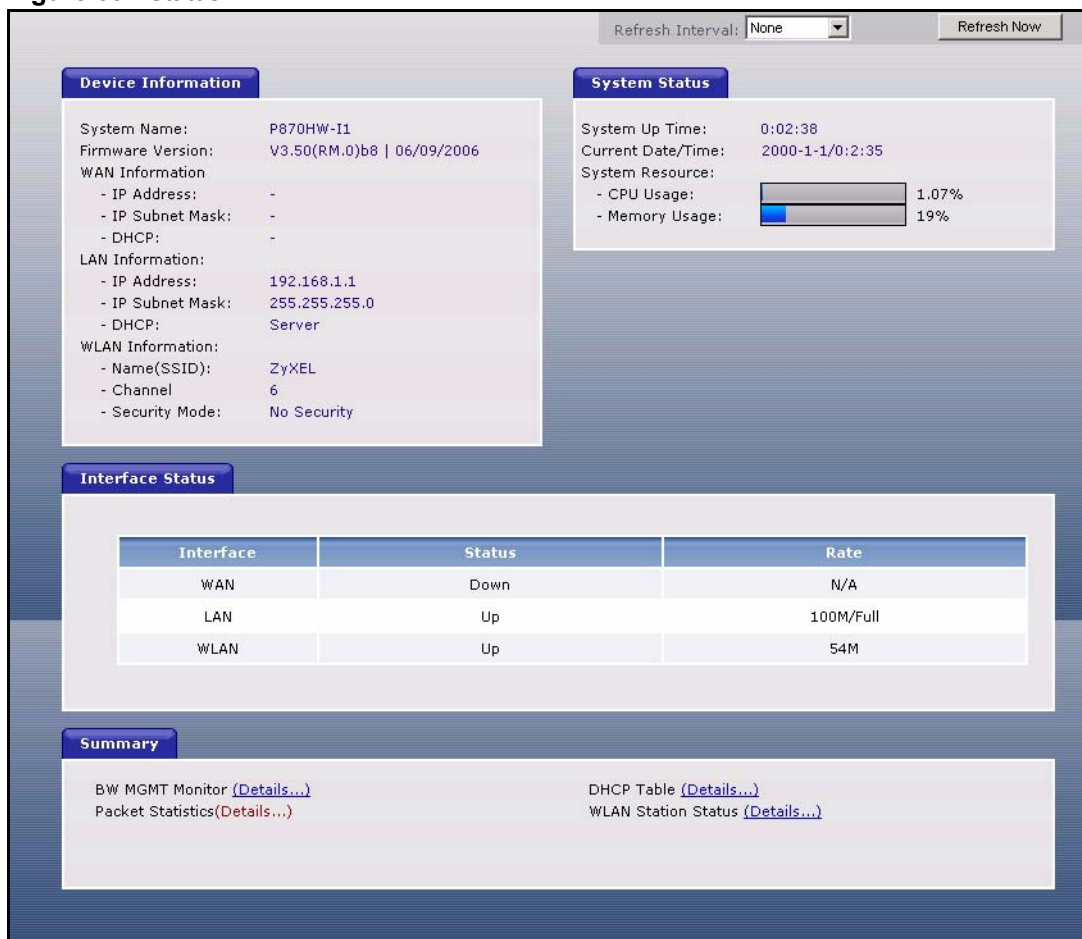
Status Screen

This chapter introduces the **Status** screen and the summary screens you can open from it.

5.1 Status Screen

To open this screen, click **Status**. This screen also appears when you log in and select **Go to Advanced setup**.

Figure 39 Status



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

Table 29 Status

LABEL	DESCRIPTION
Refresh Interval	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Refresh Now	Click this button to refresh the status screen statistics.
Device Information	
System Name	This is used for identification purposes. Click Maintenance > System > General to change it.
Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. Click Maintenance > Tools > Firmware to change it.
WAN Information	
IP Address	This is the WAN port IP address. Click Network > WAN > Internet Connection to change it.
IP Subnet Mask	This is the WAN port IP subnet mask. Click Network > WAN > Internet Connection to change it.
DHCP	This is the WAN port DHCP role - Client or None . Click Network > WAN > Internet Connection to change it.
LAN Information	
IP Address	This is the LAN port IP address. Click Network > LAN > IP to change it.
IP Subnet Mask	This is the LAN port IP subnet mask. Click Network > LAN > IP to change it.
DHCP	This is the LAN port DHCP role - Server, Relay or None . Click Network > DHCP Server > General to change it.
WLAN Information	
Name(SSID)	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN. Click Network > Wireless LAN > General to change it.
Channel	This is the channel number used by the ZyXEL Device now. Click Network > Wireless LAN > General to change it.
Security Mode	This field displays what kind of authentication and encryption the ZyXEL Device is currently using in the wireless network. Click Network > Wireless LAN > General to change it.
System Status	
System Uptime	This is the total time the ZyXEL Device has been on.
Current Date/Time	This field displays your ZyXEL Device's present date and time. Click Maintenance > System > Time Setting to change it.
System Resource	
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should use bandwidth management to turn off other applications. Click Management > Bandwidth MGMT > Configuration .

Table 29 Status

LABEL	DESCRIPTION
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. Click Maintenance > Tools > Restart, or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This field displays the ZyXEL Device ports.
Status	<p>For the WAN port, this field depends on the encapsulation.</p> <p>For Ethernet encapsulation: Down - line is down Up - line is up or connected</p> <p>For PPP over Ethernet (PPPoE) encapsulation: Down - line is down Up - line is up or connected Idle - line (ppp) idle Dial - starting to trigger a call Drop - dropping a call</p> <p>For the LAN port, this field displays one of the following values: Down - there are no LAN connections Up - line is at least one LAN connection</p> <p>For the WLAN port, this field displays one of the following values: Down - the wireless interface is disabled Up - the wireless interface is enabled</p>
Rate	<p>For the WAN port, this field displays the downstream and upstream transmission rates.</p> <p>For the LAN port, this field displays the port speed and duplex setting.</p> <p>For the WLAN port, this field displays the transmission rate.</p> <p>If any port is down or disabled, this field displays N/A.</p>
Summary	
DHCP Table	Use this screen to view current DHCP client information.
WLAN Station Status	This screen displays the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device.
BW MGMT Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Packet Statistics	Use this screen to view port status and packet specific statistics.

5.1.1 Status: BW MGMT Monitor

Use this screen to view the bandwidth usage based on the rules you configure for the LAN, WAN and WLAN. To access this screen, click **Status**, and then click **(Details...)** next to **BW MGMT Monitor**.

Figure 40 Status > BW MGMT Monitor



5.1.2 Status: DHCP Table

To access this screen, click **Status**, and then click **(Details...)** next to **DHCP Table**.

Figure 41 Status > DHCP Table

DHCP Table			
#	IP Address	Host Name	MAC Address
1	192.168.1.33	TWNB12602	00:15:00:01:1c:44
2	192.168.1.34		00:50:8d:48:59:1f
3	192.168.1.35	Joe	00:0e:9b:1b:14:55
4	192.168.1.37	TW12258-NB	00:12:f0:59:1c:92

Refresh

Each field is described in the following table.

Table 30 Status > DHCP 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 the ZyXEL Device assigned to a computer in the network.
Host Name	This field displays the system name of the computer to which the ZyXEL Device assigned the IP address.
MAC Address	This field displays the MAC address of the computer to which the ZyXEL Device assigned the IP address.
Refresh	Click this to update this screen.

5.1.3 Status: Packet Statistics

Use this screen to view the port status, packet-specific statistics, and system up time. To access this screen, click **Status**, and then click **(Details...)** next to **Packet Statistics**.

Figure 42 Status > Packet Statistics

Packet Statistics							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	2138	1656	0	0	0	0:47:12
WLAN	54M	485	730	0	0	0	0:47:11

System Up Time : 0:47:17

Poll Interval(s) : sec Set Interval Stop

The following table describes the fields in this screen.

Table 31 Status > Packet Statistics

LABEL	DESCRIPTION
Packet Statistics	
Port	This field displays the ZyXEL Device ports.
Status	This field displays the status of each ZyXEL Device port. The values are the same ones shown in the Status screen.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Collisions	This is the number of collisions on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the amount of time this port has been up.
System Up Time	This is the elapsed time the system has been up.
Poll Interval(s) Set Interval	Type how many seconds the ZyXEL Device should wait before it automatically refreshes this screen. Click Set Interval to apply the change.
Stop	Click this button to stop refreshing this screen.

5.1.4 Status: WLAN Station Status

Use this screen to view the wireless stations that are currently associated to the ZyXEL Device. To access this screen, click **Status**, and then click **(Details...)** next to **WLAN Status**.

Figure 43 Status > WLAN Station Status

Association List		
#	MAC Address	Association Time
001	00:0c:f1:32:b3:a6	00:27:25 2000/01/01
002	00:15:00:01:1c:44	00:31:22 2000/01/01
003	00:0e:9b:1b:14:55	00:33:30 2000/01/01
004	00:12:f0:58:47:81	00:36:52 2000/01/01
005	00:a0:c5:40:c2:a1	00:44:36 2000/01/01
006	00:12:f0:59:1c:92	00:42:24 2000/01/01

Refresh

The following table describes the labels in this screen.

Table 32 Status > WLAN Station Status

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
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.

CHAPTER 6

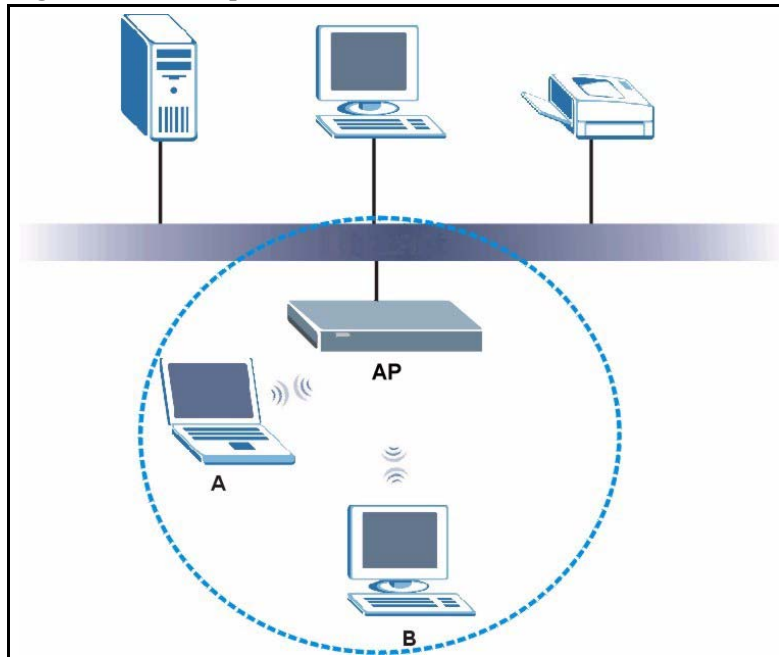
Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device.

6.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 44 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every wireless client 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 different channels.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.

Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

6.2 Wireless Security Overview

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

6.2.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP 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 devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

6.2.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

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

6.2.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

-
1. 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.
 2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized 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.

Local user databases also have an additional limitation that is explained in the next section.

6.2.4 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.

The types of encryption you can choose depend on the type of user authentication. (See [Section 6.2.3 on page 94](#) for information about this.)

Table 33 Types of Encryption for Each Type of User Authentication

	No Authentication	RADIUS Server
Weakest	None	IEEE 802.1x + No WEP
↕	Static WEP	IEEE 802.1x + Static WEP
		IEEE 802.1x + Dynamic WEP
	WPA-PSK	WPA
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **IEEE 802.1x**, **IEEE 802.1x + Static WEP**, **IEEE 802.1x + Dynamic WEP**, **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 wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. 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. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized 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 wireless clients 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 wireless client in the wireless network must have the same key.

6.2.5 One-Touch Intelligent Security Technology (OTIST)

With ZyXEL's OTIST, you set up the SSID and the encryption (WEP or WPA-PSK) on the ZyXEL Device. Then, the ZyXEL Device transfers them to wireless clients in the wireless network. As a result, you do not have to set up the SSID and encryption on every wireless client.

The wireless clients 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 6.5 on page 108](#) for more details.

6.3 Wireless Performance Overview

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

6.3.1 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 large file downloads so that they do not reduce the quality of other applications.

6.4 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 click **Apply**. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

To open this screen, click **Network > Wireless LAN**.

Figure 45 Network > Wireless LAN > General

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

Table 34 Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	Enter the name of the wireless network. The name is called the Service Set IDentity (SSID). Every wireless client in the same wireless network must use the same SSID. Note: If you are using the wireless network to connect to the ZyXEL Device from a computer and you change this setting, you will lose your wireless connection when you press Apply to confirm. You must change the wireless settings of your computer to match the ZyXEL Device's new settings.
Hide SSID	Select this check box to hide the SSID so a station cannot get the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency or channel your wireless network uses. It should be at least five channels away from other wireless networks in the area.
Security	This section is described in more detail below.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

6.4.1 General Wireless LAN Screen: No Security

Use this screen to allow wireless stations to communicate with the access points without any data encryption. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **No Security**.

Note: 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.

Figure 46 Network > Wireless LAN > General > No Security

The following table describes the labels in this screen.

Table 35 Network > Wireless LAN > General > No Security

LABEL	DESCRIPTION
Security Mode	Select No Security .

6.4.2 General Wireless LAN Screen: Static WEP

Use this screen to enable and configure WEP encryption in your wireless network. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **No Security**.

Figure 47 Network > Wireless LAN > General > Static WEP

The following table describes the labels in this screen.

Table 36 Network > Wireless LAN > General > Static WEP

LABEL	DESCRIPTION
Security Mode	Select Static WEP .
WEP Key	Enter the key you want to use. You can enter the key using printable ASCII characters or hexadecimal (0-9, A-F, a-f) characters. The ZyXEL Device and the wireless stations must use the same WEP key. If you want to use a 64-bit WEP key, enter 5 printable ASCII characters or 10 hexadecimal characters. If you want to use a 128-bit WEP key, enter 13 printable ASCII characters or 26 hexadecimal characters. A 128-bit WEP key is more secure than a 64-bit WEP key.

6.4.3 General Wireless LAN Screen: WPA-PSK

Use this screen to enable and configure WPA-PSK encryption in your wireless network. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **WPA-PSK**.

Figure 48 Network > Wireless LAN > General > WPA-PSK

The following table describes the labels in this screen.

Table 37 Network > Wireless LAN > General > WPA-PSK

LABEL	DESCRIPTION
Security Mode	Select WPA-PSK .
Pre-Shared Key	Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). The key is case-sensitive.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.

Table 37 Network > Wireless LAN > General > WPA-PSK (continued)

LABEL	DESCRIPTION
Idle Timeout	<p>The ZyXEL Device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to enter the username and password again before it can use the wireless network again. Some wireless clients can do this automatically; some wireless clients cannot, in which case the user has to enter the information again. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.</p> <p>Enter a time interval between 10 and 9999 seconds. 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 minimize the number of delays caused by logging in again.</p>
Group Key Update Timer	<p>The Group Key Update Timer is the rate at which the ZyXEL Device sends a new group key to all clients. This process changes the WEP key on a regular basis. Enter a time interval between 10 and 9999 seconds.</p>

6.4.4 General Wireless LAN Screen: WPA

Use this screen to enable and configure WPA encryption in your wireless network. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **WPA**.

Figure 49 Network > Wireless LAN > General > WPA

The screenshot displays the configuration interface for WPA encryption. It is divided into two main sections: 'Wireless Setup' and 'Security'. In the 'Wireless Setup' section, 'Enable Wireless LAN' is checked, the SSID is 'ZyXEL', 'Hide SSID' is unchecked, and the channel is set to 'Channel-06 2437Mhz'. The 'Security' section shows 'Security Mode' set to 'WPA'. Three timers are configured: 'ReAuthentication Timer' at 1800 seconds, 'Idle Timeout' at 3600 seconds, and 'Group Key Update Timer' at 1800 seconds. Below these are fields for an 'Authentication Server' (IP: 0.0.0.0, Port: 1812, Shared Secret) and an 'Accounting Server' (Active: unchecked, IP: 0.0.0.0, Port: 1813, Shared Secret). At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 38 Network > Wireless LAN > General > WPA

LABEL	DESCRIPTION
Security Mode	Select WPA .
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.
Idle Timeout	<p>The ZyXEL Device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to enter the username and password again before it can use the wireless network again. Some wireless clients can do this automatically; some wireless clients cannot, in which case the user has to enter the information again. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.</p> <p>Enter a time interval between 10 and 9999 seconds. 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 minimize the number of delays caused by logging in again.</p>
Group Key Update Timer	The Group Key Update Timer is the rate at which the ZyXEL Device sends a new group key to all clients. This process changes the WEP key on a regular basis. Enter a time interval between 10 and 9999 seconds.
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. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Enter a password (up to 31 alphanumeric characters) to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server. The key is not sent over the network.
Accounting Server	These settings are optional.
Active	Select this 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. You need not change this value unless your network administrator instructs you to do so.
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. The key is not sent over the network.

6.4.5 General Wireless LAN Screen: 802.1x + Dynamic WEP

Use this screen to enable and configure IEEE 802.1x authentication and dynamic WEP encryption in your wireless network. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **802.1x + Dynamic WEP**.

Figure 50 Network > Wireless LAN > General > 802.1x + Dynamic WEP

The following table describes the labels in this screen.

Table 39 Network > Wireless LAN > General > 802.1x + Dynamic WEP

LABEL	DESCRIPTION
Security Mode	Select 802.1x + Dynamic WEP .
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. Enter a time interval between 10 and 9999 seconds.
Dynamic WEP Key Exchange	Select the length of the keys. The longer the key, the stronger the security, but also the more processing is required.
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. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Enter a password (up to 31 alphanumeric characters) to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server. The key is not sent over the network.
Accounting Server	These settings are optional.
Active	Select this to enable user accounting through an external authentication server.

Table 39 Network > Wireless LAN > General > 802.1x + Dynamic WEP (continued)

LABEL	DESCRIPTION
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. You need not change this value unless your network administrator instructs you to do so.
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. The key is not sent over the network.

6.4.6 General Wireless LAN Screen: 802.1x + Static WEP

Use this screen to enable and configure IEEE 802.1x authentication and static WEP encryption in your wireless network. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **802.1x + Static WEP**.

Figure 51 Network > Wireless LAN > General > 802.1x + Static WEP

Wireless Setup

Enable Wireless LAN

Name(SSID)

Hide SSID

Channel Selection

Security

Security Mode

WEP Key

Note:
 The different WEP key lengths configure different strength security, 40/64-bit, or 104/128-bit respectively. Your wireless client must match the security strength set on the router.
 -Please type exactly 5, or 13 characters.
 -Please type exactly 10, or 26 characters using only the numbers 0-9 and the letters A-F.

ReAuthentication Timer (In Seconds)

Idle Timeout (In Seconds)

Authentication Server

 IP Address

 Port Number

 Shared Secret

Accounting Server

Active

 IP Address

 Port Number

 Shared Secret

The following table describes the labels in this screen.

Table 40 Network > Wireless LAN > General > 802.1x + Static WEP

LABEL	DESCRIPTION
Security Mode	Select 802.1x + Static WEP .
WEP Key	Enter the key you want to use. You can enter the key using printable ASCII characters or hexadecimal (0-9, A-F, a-f) characters. The ZyXEL Device and the wireless stations must use the same WEP key. If you want to use a 64-bit WEP key, enter 5 printable ASCII characters or 10 hexadecimal characters. If you want to use a 128-bit WEP key, enter 13 printable ASCII characters or 26 hexadecimal characters. A 128-bit WEP key is more secure than a 64-bit WEP key.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to enter the username and password again before it can use the wireless network again. Some wireless clients can do this automatically; some wireless clients cannot, in which case the user has to enter the information again. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. Enter a time interval between 10 and 9999 seconds. 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 minimize the number of delays caused by logging in again.
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. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Enter a password (up to 31 alphanumeric characters) to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server. The key is not sent over the network.
Accounting Server	These settings are optional.
Active	Select this 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. You need not change this value unless your network administrator instructs you to do so.
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. The key is not sent over the network.

6.4.7 General Wireless LAN Screen: 802.1x + No WEP

Use this screen to enable and configure IEEE 802.1x authentication without WEP encryption in your wireless network. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **802.1x + No WEP**.

Figure 52 Network > Wireless LAN > General > 802.1x + No WEP

The following table describes the labels in this screen.

Table 41 Network > Wireless LAN > General > 802.1x + No WEP

LABEL	DESCRIPTION
Security Mode	Select 802.1x + No WEP .
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to enter the username and password again before it can use the wireless network again. Some wireless clients can do this automatically; some wireless clients cannot, in which case the user has to enter the information again. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. Enter a time interval between 10 and 9999 seconds. 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 minimize the number of delays caused by logging in again.
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. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Enter a password (up to 31 alphanumeric characters) to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server. The key is not sent over the network.

Table 41 Network > Wireless LAN > General > 802.1x + No WEP (continued)

LABEL	DESCRIPTION
Accounting Server	These settings are optional.
Active	Select this 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. You need not change this value unless your network administrator instructs you to do so.
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. The key is not sent over the network.

6.4.8 General Wireless LAN Screen: WPA2-PSK

Use this screen to enable and configure WPA2-PSK encryption in your wireless network. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **WPA2-PSK**.

Figure 53 Network > Wireless LAN > General > WPA2-PSK

The screenshot shows the configuration interface for WPA2-PSK. It is divided into two main sections: 'Wireless Setup' and 'Security'. In the 'Wireless Setup' section, 'Enable Wireless LAN' is checked, the SSID is 'ZyXEL', 'Hide SSID' is unchecked, and the channel is set to 'Channel-06 2437MHz'. The 'Security' section shows 'Security Mode' set to 'WPA2-PSK', 'WPA Compatible' is unchecked, and the 'Pre-Shared Key' field is empty. Three timer fields are present: 'ReAuthentication Timer' (1800), 'Idle Timeout' (3600), and 'Group Key Update Timer' (1800), all measured in seconds. 'Apply' and 'Reset' buttons are located at the bottom of the form.

The following table describes the labels in this screen.

Table 42 Network > Wireless LAN > General > WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Select WPA2-PSK .
WPA Compatible	Select this if the ZyXEL Device should be able to handle WPA-PSK and WPA2-PSK, depending on the abilities of each wireless station. This requires additional processing and may reduce throughput.
Pre-Shared Key	Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). The key is case-sensitive.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.

Table 42 Network > Wireless LAN > General > WPA2-PSK (continued)

LABEL	DESCRIPTION
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. Enter a time interval between 10 and 9999 seconds.
Group Key Update Timer	The Group Key Update Timer is the rate at which the ZyXEL Device sends a new group key to all clients. This process changes the WEP key on a regular basis. Enter a time interval between 10 and 9999 seconds.

6.4.9 General Wireless LAN Screen: WPA2

Use this screen to enable and configure WPA2 encryption in your wireless network. To open this screen, click **Network > Wireless LAN**, and set **Security Mode** to **WPA2**.

Figure 54 Network > Wireless LAN > General > WPA2

Wireless Setup

- Enable Wireless LAN
- Name(SSID):
- Hide SSID
- Channel Selection:

Security

- Security Mode:
- WPA Compatible
- ReAuthentication Timer: (In Seconds)
- Idle Timeout: (In Seconds)
- Group Key Update Timer: (In Seconds)
- Authentication Server
 - IP Address:
 - Port Number:
 - Shared Secret:
- Accounting Server
 - Active
 - IP Address:
 - Port Number:
 - Shared Secret:

The following table describes the labels in this screen.

Table 43 Network > Wireless LAN > General > WPA2

LABEL	DESCRIPTION
Security Mode	Select WPA2 .
WPA Compatible	Select this if the ZyXEL Device should be able to handle WPA-PSK and WPA2-PSK, depending on the abilities of each wireless station. This requires additional processing and may reduce throughput.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. Enter a time interval between 10 and 9999 seconds.
Group Key Update Timer	The Group Key Update Timer is the rate at which the ZyXEL Device sends a new group key to all clients. This process changes the WEP key on a regular basis. Enter a time interval between 10 and 9999 seconds.
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. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Enter a password (up to 31 alphanumeric characters) to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server. The key is not sent over the network.
Accounting Server	These settings are optional.
Active	Select this 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. You need not change this value unless your network administrator instructs you to do so.
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. The key is not sent over the network.

6.5 OTIST Screen

Use this screen to set up and start OTIST on the ZyXEL Device in your wireless network. To open this screen, click **Network > Wireless LAN > OTIST**.

Figure 55 Network > Wireless LAN > OTIST

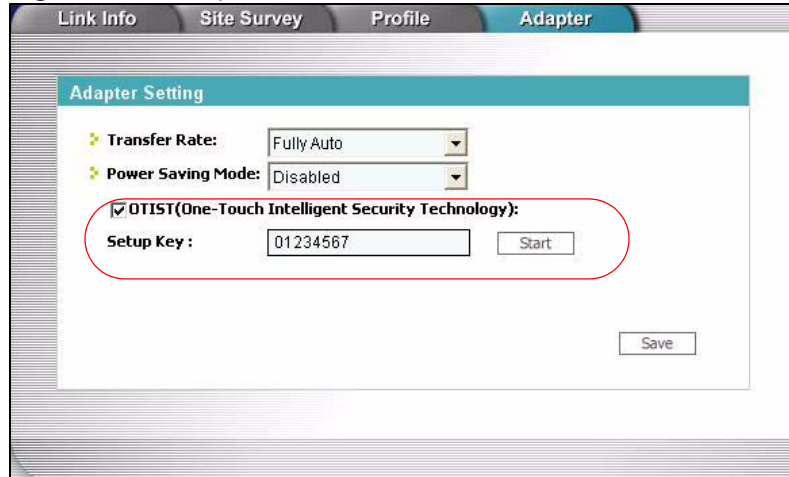
The following table describes the labels in this screen.

Table 44 Network > Wireless LAN > OTIST

LABEL	DESCRIPTION
Setup Key	Type a key (password) 8 ASCII characters long. Note: If you change the OTIST setup key in the ZyXEL Device, you must change it on the wireless clients too.
Yes!	Select this if you want the ZyXEL Device to automatically generate a pre-shared key for the wireless network. Before you do this, click Network > Wireless LAN > General and set the Security Mode to No Security . Clear this if you want the ZyXEL Device to use a pre-shared key that you enter. Before you do this, click Network > Wireless LAN > General , set the Security Mode to WPA-PSK , and enter the Pre-Shared Key .
Start	Click Start to activate OTIST and transfer settings. The process takes three minutes to complete. Note: You must click Start in the ZyXEL Device and in the wireless client(s) within three minutes of each other. You can start OTIST in the wireless clients and the ZyXEL Device in any order.

Before you click **Start**, you should enable OTIST on all the OTIST-enabled wireless clients in the wireless network. For most wireless clients, follow these steps.

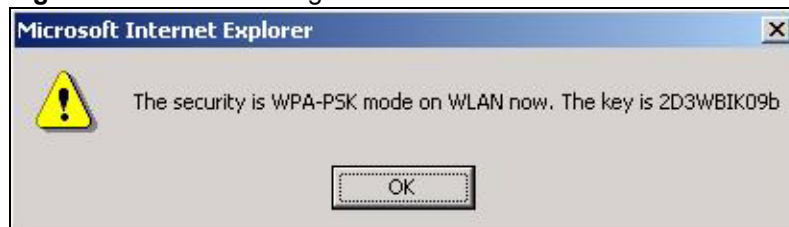
- 1 Start the ZyXEL utility
- 2 Click the **Adapter** tab.
- 3 Select the **OTIST** check box, and enter the same **Setup Key** as the ZyXEL Device.
- 4 Click **Save**.

Figure 56 Example: Wireless Client OTIST Screen

To start OTIST in the wireless client, click **Start** in this screen.

Note: You must click **Start** in the ZyXEL Device and in the wireless client(s) within three minutes of each other. You can start OTIST in the wireless clients and the ZyXEL Device in any order.

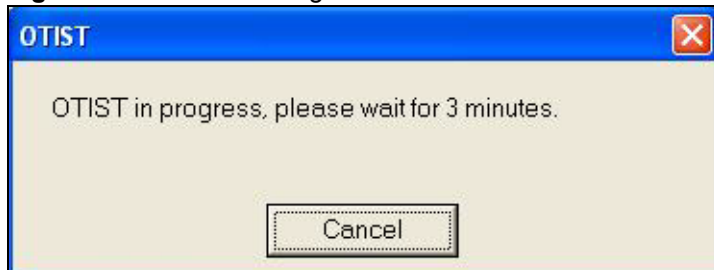
After you click **Start** in the ZyXEL Device, the following screen appears (in the ZyXEL Device).

Figure 57 OTIST: Settings

You can use the key in this screen to set up WPA-PSK encryption manually for non-OTIST wireless clients in the wireless network.

Review the settings, and click **OK**. The ZyXEL Device begins transferring OTIST settings. The following screens appear in the ZyXEL Device and in the wireless clients.

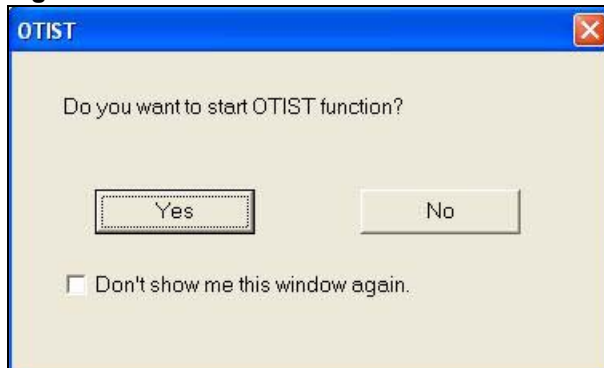
Figure 58 OTIST: In Progress on the ZyXEL Device

Figure 59 OTIST: In Progress on the Wireless Client

These screens close when the transfer is complete.

6.5.1 Notes on OTIST

- 1 If you enable OTIST in a wireless client, you see this screen each time you start the utility. Click **Yes** to search for an OTIST-enabled AP (in other words, the ZyXEL Device).

Figure 60 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 After the wireless client finds an OTIST-enabled AP, you must click **Start** in the ZyXEL Device's **Network > Wireless LAN > OTIST** screen or hold in the **Reset** button on the ZyXEL Device for one or two seconds to transfer the settings again.
- 4 If you change the SSID or the keys on the ZyXEL Device 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 OTIST-enabled wireless client joins your wireless network, you need to run OTIST on the AP and ALL wireless clients again.

6.6 MAC Filter Screen

Use this screen to enable and configure MAC filtering in your wireless network. To open this screen, click **Network > Wireless LAN > MAC Filter**.

Figure 61 Network > Wireless LAN > MAC Filter

MAC Address Filter

Active

Filter Action Allow Deny

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

The following table describes the labels in this menu.

Table 45 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Select this to enable MAC address filtering.
Filter Action	Define the filter action for the MAC addresses in the MAC Address table. Select Deny to stop these MAC addresses from accessing the ZyXEL Device. Other MAC address are allowed to access the ZyXEL Device. Select Allow to allow these MAC addresses to access the ZyXEL Device. Other MAC addresses are not allowed to access the ZyXEL Device.
Set	This is a sequential value, and it is not associated with a specific MAC address.
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in the format shown.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

6.7 Advanced Wireless LAN Screen

Use this screen to enable and configure roaming and other advanced wireless settings in your wireless network. To open this screen, click **Network > Wireless LAN > Advanced**.

Figure 62 Network > Wireless LAN > Advanced

The following table describes the labels in this screen.

Table 46 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Roaming Configuration	
Enable Roaming	If you have two or more APs on your wireless network, you can enable this option so that wireless clients can change locations without having to log in again. This is useful for wireless clients, such as notebooks, that move around a lot.
Port	Enter the UDP port number the APs use to communicate with each other. All of the APs in your wireless network must use the same UDP port number. Enter a value between 1 and 65535.
Wireless Advanced Setup	
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: Long and Short . Most wireless clients can detect the AP's preamble automatically. However, if a wireless client tries to use a different preamble mode than the AP does, it cannot communicate with the AP. Select Dynamic if you want the AP to support both modes.
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 both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

CHAPTER 7

WAN

This chapter describes how to configure outside connections to another network or the Internet.

7.1 WAN Overview

7.1.1 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 the idle timeout is disabled. The second is that the ZyXEL Device automatically tries to bring up the connection when it is turned on or when the connection is down. Do not set up a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

7.1.2 Metric

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

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

- Normal route: designated by the ISP (see [Section 7.2 on page 120](#))
- Traffic-redirect route (see [Section 7.4 on page 124](#))

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2", 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.

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

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

7.2 Internet Connection Screens

This screen depends on the **Encapsulation** your ISP uses.

7.2.1 Internet Connection Screen: Ethernet

Use this screen to set up an Ethernet connection to the Internet. To open this screen, click **Network > WAN > Internet Connection**, and set the **Encapsulation** to **Ethernet**.

Figure 63 Network > WAN > Internet Connection > Ethernet

The following table describes the labels in this screen.

Table 47 Network > WAN > Internet Connection > Ethernet

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select Ethernet .
WAN IP Address Assignment	
Get automatically from ISP	Select this if your ISP did not give you a fixed (static) IP address. Do not enter anything in the IP Address , IP Subnet Mask or Gateway IP Address fields.
Use Fixed IP Address	Select this if your ISP gave you a fixed (static) IP address.
IP Address	Enter the fixed (static) IP address provided by your ISP.
IP Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the IP address of the gateway provided by your ISP.
WAN MAC Address	

Table 47 Network > WAN > Internet Connection > Ethernet (continued)

LABEL	DESCRIPTION
Spoof WAN MAC Address	Select this if you want the ZyXEL Device to use the MAC address of another computer, instead of its default MAC address. You might try this if you lose your Internet connection because some ISPs check the MAC address of the device connected to the Internet.
IP Address	If you select Spoof WAN MAC Address , enter the IP address of the computer whose MAC address you want the ZyXEL Device to use. This is usually a computer on the LAN.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

7.2.2 Internet Connection Screen: PPP over Ethernet (PPPoE)

Use this screen to set up a PPP over Ethernet (PPPoE) connection to the Internet. To open this screen, click **Network > WAN > Internet Connection**, and set the **Encapsulation** to **PPP over Ethernet**.

Figure 64 Network > WAN > Internet Connection > PPP over Ethernet

The screenshot shows the configuration interface for an Internet Connection. At the top, there are tabs for 'Internet Connection', 'Advanced', and 'Traffic Redirect'. The main content is organized into three sections:

- ISP Parameters for Internet Access:**
 - Encapsulation: PPP over Ethernet (dropdown)
 - Service Name: (optional) (text input)
 - User Name: (text input)
 - Password: (password input)
 - Retype to Confirm: (password input)
 - Nailed-Up Connection
 - Idle Timeout (sec): 100 (in seconds)
- WAN IP Address Assignment:**
 - Get automatically from ISP (Default)
 - Use Fixed IP Address
 - My WAN IP Address: 0.0.0.0
 - Metric: 1
 - Private: No (dropdown)
- WAN MAC Address:**
 - Spoof WAN MAC Address
 - Clone the computer's MAC address - IP Address: 192.168.1.34

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

The following table describes the labels in this screen.

Table 48 Network > WAN > Internet Connection > PPP over Ethernet

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select PPP over Ethernet .
Service Name	Enter the service name provided by your ISP. Leave this field blank if your ISP did not provide one.
User Name	Enter the user name provided by your ISP.
Password	Enter the password provided by your ISP.
Retype to Confirm	Enter the password again.
Nailed-Up Connection	Select this if you want the ZyXEL Device to automatically connect to your ISP when it is turned on and to remain connected all the time. This is not recommended if you pay for your Internet connected based on the amount of time you are connected.
Idle Timeout (sec)	Enter the number of seconds the ZyXEL Device should wait while there is no Internet traffic before it automatically disconnects from the ISP. Enter a time interval between 10 and 9999 seconds.
WAN IP Address Assignment	
Get automatically from ISP	Select this if your ISP did not give you a fixed (static) IP address. Do not enter anything in the My WAN IP Address field.
Use Fixed IP Address	Select this if your ISP gave you a fixed (static) IP address.
My WAN IP Address	Enter the fixed (static) IP address provided by your ISP.
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".
Private	This field is related to RIP. This field determines whether or not the ZyXEL Device includes the route to this remote node in its RIP broadcasts. If you select Yes , this route is not included in RIP broadcast. If you select No , the route to this remote node is propagated to other hosts through RIP broadcasts. Usually, you should keep the default value.
WAN MAC Address	
Spoof WAN MAC Address	Select this if you want the ZyXEL Device to use the MAC address of another computer, instead of its default MAC address. You might try this if you lose your Internet connection because some ISPs check the MAC address of the device connected to the Internet.
IP Address	If you select Spoof WAN MAC Address , enter the IP address of the computer whose MAC address you want the ZyXEL Device to use. This is usually a computer on the LAN.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

7.3 Advanced WAN Screen

Use this screen to edit the advanced settings for your Internet connection. To open this screen, click **Network > WAN > Advanced**.

Figure 65 Network > WAN > Advanced

The following table describes the labels in this screen.

Table 49 Network > WAN > Advanced

LABEL	DESCRIPTION
DNS Servers	DNS (Domain Name System) manages the relationships between domain names and IP addresses. For example, the IP address of www.zyxel.com is 204.217.0.2. Without a DNS server, you must know the IP address of the computer you want to access before you access it.
First DNS Server Second DNS Server Third DNS Server	Select From ISP if your ISP dynamically assigns DNS server information. (In this case, the ISP assigns the WAN IP address too. See Network > WAN > Internet Connection .) The field to the right is read-only, and it displays the IP address provided by your ISP. Select User-Defined if you have the IP address of a DNS server. You might get it from your ISP or from your network. Enter the IP address in the field to the right. Select None if you do not want to use this DNS server. If you select None for all of the DNS servers, you must use IP addresses to configure the ZyXEL Device and to access the Internet.
RIP & Multicast Setup	

Table 49 Network > WAN > Advanced (continued)

LABEL	DESCRIPTION
RIP Direction	<p>Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet.</p> <p>None - The ZyXEL Device does not send or receive routing information on the subnet.</p> <p>Both - The ZyXEL Device sends and receives routing information on the subnet.</p> <p>In Only - The ZyXEL Device only receives routing information on the subnet.</p> <p>Out Only - The ZyXEL Device only sends routing information on the subnet.</p>
RIP Version	<p>Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet.</p> <p>RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information.</p> <p>RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information.</p> <p>RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.</p>
Multicast	<p>Select which version of IGMP the ZyXEL Device uses to support multicasting on the WAN. Multicasting sends packets to some computers on the WAN and is an alternative to unicasting (sending packets to one computer) and broadcasting (sending packets to every computer).</p> <p>None - The ZyXEL Device does not support multicasting.</p> <p>IGMP-v1 - The ZyXEL Device supports IGMP version 1.</p> <p>IGMP-v2 - The ZyXEL Device supports IGMP version 2.</p> <p>Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers on the WAN have to support the same version of IGMP.</p>
Windows Networking	
Allow between LAN and WAN	<p>Select this check box if you want the ZyXEL Device to send NetBIOS (Network Basic Input/Output System) packets between the LAN and WAN. You should also make sure that NetBIOS packets are not blocked in Security > Firewall > Rules.</p> <p>NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with computers on other networks. It may sometimes be necessary to allow NetBIOS packets to pass through the ZyXEL Device in order to allow computers on the LAN to find computers on the WAN and vice versa.</p> <p>This is the same setting you can set in Network > LAN > Advanced.</p>
Allow Trigger Dial	Select this if you want to allow NetBIOS packets to initiate calls.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

7.4 Traffic Redirect Screen

Use this screen to specify a backup gateway in case the default gateway (your ISP) is not available. (If you do not have a backup gateway, do not use this screen.) To access this screen, click **Network > WAN > Traffic Redirect**.

Figure 66 Network > WAN > Traffic Redirect

The screenshot shows the 'Traffic Redirect' configuration page. At the top, there are three tabs: 'Internet Connection', 'Advanced', and 'Traffic Redirect'. The 'Traffic Redirect' tab is selected. Below the tabs, the page title is 'Traffic Redirect'. There is a checkbox labeled 'Active'. Below it are several input fields: 'Backup Gateway IP Address' with the value '0.0.0.0', 'Check WAN IP Address' with the value '0.0.0.0', 'Fail Tolerance' with the value '2', 'Period (sec)' with the value '5' and '(in seconds)' to its right, and 'Timeout (sec)' with the value '3' and '(in seconds)' to its right. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 50 Network > WAN > Traffic Redirect

LABEL	DESCRIPTION
Active	Select this to set up a backup gateway in case the default gateway is not available. (For example, this might happen if the Internet connection goes down.) Clear this if you do not have a backup gateway.
Backup Gateway IP Address	Enter the IP address of the backup gateway. The ZyXEL Device automatically uses this gateway if the default gateway is not available anymore.
Check WAN IP Address	Enter the IP address of a reliable nearby computer the ZyXEL Device uses to test whether or not the default gateway is available anymore. For example, use one of your ISP's DNS server addresses. If you enter 0.0.0.0, the test fails every time.
Fail Tolerance	Enter the number of consecutive times the ZyXEL Device may attempt and fail to find the reliable nearby computer at Check WAN IP Address before it starts using the backup gateway. 2-5 are typical choices.
Period (sec)	Enter the number of seconds between attempts to find the reliable nearby computer at Check WAN IP Address . 5 - 60 are typical choices.
Timeout (sec)	Enter the number of seconds the ZyXEL Device waits for a response from the reliable nearby computer at Check WAN IP Address before the attempt is a failure. 3-50 are typical choices, but this number should be less than the Period .
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

CHAPTER 8

LAN

This chapter describes how to configure settings for the LAN port.

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.

8.1.1 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. Otherwise, it is recommended that you pick an IP address between 192.168.0.0 to 192.168.255.255 and that no other device on your network is using; for example, 192.168.1.1.

Your ZyXEL Device automatically computes the subnet mask based on the IP address that you entered. You should not change it unless you are instructed to do so.

8.1.2 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.

8.1.3 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.

8.1.4 LAN IP Alias

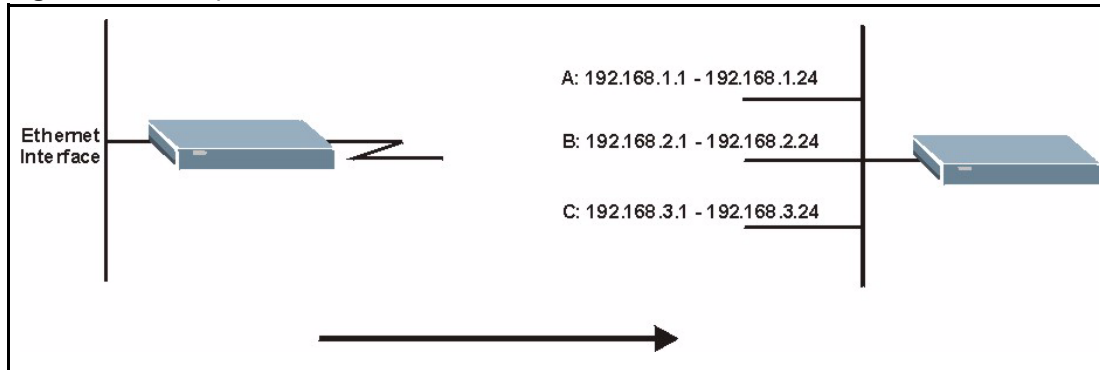
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

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.

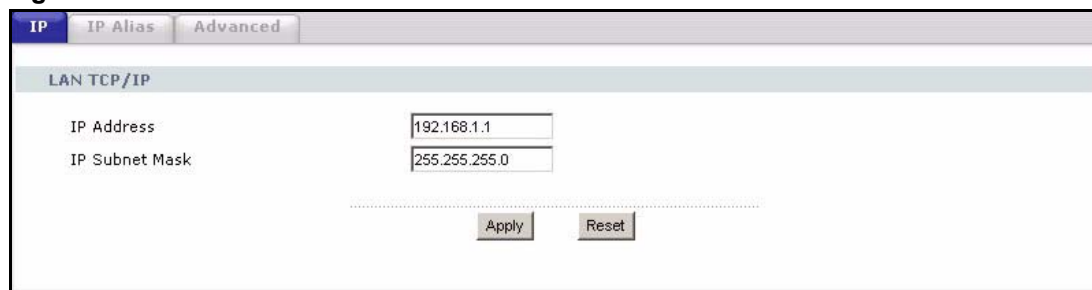
Figure 67 Example: IP Alias



8.2 LAN IP Screen

Use this screen to set up the IP address and subnet mask of your LAN port. To open this screen, click **Network > LAN > IP**.

Figure 68 Network > LAN > IP



The following table describes the fields in this screen.

Table 51 Network > 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 or network administrator. If they did not provide one, use the default value.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

8.3 LAN IP Alias Screen

Use this screen to set up additional subnets (logical networks) on your LAN port. To open this screen, click **Network > LAN > IP Alias**.

Figure 69 Network > LAN > IP Alias

The following table describes the fields in this screen.

Table 52 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1	
IP Alias 1	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the ZyXEL Device on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. None - The ZyXEL Device does not send or receive routing information on the subnet. Both - The ZyXEL Device sends and receives routing information on the subnet. In Only - The ZyXEL Device only receives routing information on the subnet. Out Only - The ZyXEL Device only sends routing information on the subnet.
RIP Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information. RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information. RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.
IP Alias 2	
IP Alias 2	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the ZyXEL Device on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.

Table 52 Network > LAN > IP Alias (continued)

LABEL	DESCRIPTION
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. None - The ZyXEL Device does not send or receive routing information on the subnet. Both - The ZyXEL Device sends and receives routing information on the subnet. In Only - The ZyXEL Device only receives routing information on the subnet. Out Only - The ZyXEL Device only sends routing information on the subnet.
RIP Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information. RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information. RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

8.4 Advanced LAN Screen

Use this screen to edit advanced settings, such as RIP and multicast, on the LAN port. To open this screen, click **Network > LAN > Advanced**.

Figure 70 Network > LAN > Advanced

The screenshot shows the 'Advanced' configuration screen for an IP Alias. At the top, there are three tabs: 'IP', 'IP Alias', and 'Advanced', with 'Advanced' being the active tab. Below the tabs is a section titled 'RIP & Multicast Setup'. This section contains three rows of settings, each with a label and a dropdown menu: 'RIP Direction' is set to 'Both', 'RIP Version' is set to 'RIP-1', and 'Multicast' is set to 'None'. Below this is another section titled 'Windows Networking (NetBIOS over TCP/IP)'. This section contains a single checkbox labeled 'Allow between LAN and WAN', which is checked. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the fields in this screen.

Table 53 Network > LAN > Advanced

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet.</p> <p>None - The ZyXEL Device does not send or receive routing information on the subnet.</p> <p>Both - The ZyXEL Device sends and receives routing information on the subnet.</p> <p>In Only - The ZyXEL Device only receives routing information on the subnet.</p> <p>Out Only - The ZyXEL Device only sends routing information on the subnet.</p>
RIP Version	<p>Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet.</p> <p>RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information.</p> <p>RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information.</p> <p>RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.</p>
Multicast	<p>You do not have to enable multicasting to use RIP-2M. (See RIP Version.)</p> <p>Select which version of IGMP the ZyXEL Device uses to support multicasting on the LAN. Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).</p> <p>None - The ZyXEL Device does not support multicasting.</p> <p>IGMP-v1 - The ZyXEL Device supports IGMP version 1.</p> <p>IGMP-v2 - The ZyXEL Device supports IGMP version 2.</p> <p>Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers on the LAN have to support the same version of IGMP.</p>
Windows Networking	
Allow between LAN and WAN	<p>Select this check box if you want the ZyXEL Device to send NetBIOS (Network Basic Input/Output System) packets between the LAN and WAN. You should also make sure that NetBIOS packets are not blocked in Security > Firewall > Rules.</p> <p>NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with computers on other networks. It may sometimes be necessary to allow NetBIOS packets to pass through the ZyXEL Device in order to allow computers on the LAN to find computers on the WAN and vice versa.</p> <p>This is the same setting you can set in Network > WAN > Advanced.</p>
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

CHAPTER 9

DHCP Server

This chapter describes how to configure the DHCP server for the LAN and WLAN ports.

9.1 DHCP Overview

Dynamic Host Configuration Protocol (DHCP, RFC 2131, RFC 2132) provides a way to automatically set up and maintain IP addresses, subnet masks, gateways, and some network information (such as the IP addresses of DNS servers) on computers in the network. This reduces the amount of manual configuration you have to do and usually uses available IP addresses more efficiently.

In DHCP, every network has at least one DHCP server. When a computer (a DHCP client) joins the network, it submits a DHCP request. The DHCP servers get the request; assign an IP address; and provide the IP address, subnet mask, gateway, and available network information to the DHCP client. When the DHCP client leaves the network, the DHCP servers can assign its IP address to another DHCP client.

The ZyXEL Device can be a DHCP server.¹ In this case, it provides the following information to DHCP clients.

- IP address - If the DHCP client's MAC address is in the ZyXEL Device's static DHCP table, the ZyXEL Device assigns the corresponding IP address. If not, the ZyXEL Device assigns IP addresses from a pool, defined by the starting address of the pool and the pool size.

Table 54 Example: Assigning IP Addresses from a Pool

START IP ADDRESS	POOL SIZE	RANGE OF ASSIGNED IP ADDRESS
50.50.50.33	5	50.50.50.33 - 50.50.50.37
75.75.75.1	200	75.75.75.1 - 75.75.75.200
120.120.120.100	100	120.120.120.100 - 120.120.120.199

- Subnet mask - The ZyXEL Device provides the same subnet mask you specify for the LAN port. See **Network > LAN > IP**.
- Gateway - The gateway is the ZyXEL Device, so it provides the IP address you specify for you specify for the LAN port. See **Network > LAN > IP**.

1. At the time of writing, the DHCP server is turned on by default.

- DNS servers - The ZyXEL Device provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to the DNS servers the ZyXEL Device received from the ISP.

9.2 General DHCP Screen

Use this screen to enable and configure the DHCP server for the **LAN** and **WLAN** ports. To open this screen, click **Network > DHCP Server > General**.

Figure 71 Network > DHCP Server > General

The following table describes the labels in this screen.

Table 55 Network > DHCP Server > General

LABEL	DESCRIPTION
DHCP Setup	
Enable DHCP Server	Select this to let the ZyXEL Device assign IP addresses and provides subnet mask, gateway, and DNS server information to the network. If you clear this, there should be another DHCP server on the network, or this information must be set up manually on each computer on the network.
IP Pool Starting Address	Enter the IP address from which the ZyXEL Device begins allocating IP addresses. You can assign a static IP address to a specific computer; see Network > DHCP Server > Static DHCP .
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the subnet mask 255.255.255.0. For example, if the IP Pool Start Address is 10.10.10.10, the ZyXEL Device can allocate up to 10.10.10.254, or 245 IP addresses.
DNS Server	The ZyXEL Device provides the following DNS servers to DHCP clients.

Table 55 Network > DHCP Server > General (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses of a maximum of three DNS servers that the network can use. The ZyXEL Device provides these IP addresses to DHCP clients. You can specify these IP addresses the following ways: From ISP - use the IP address of the corresponding DNS server specified in Network > WAN > Advanced . User-Defined - enter a static IP address. DNS Relay - use the ZyXEL Device's IP address. In this case, the ZyXEL Device finds out the IP address of the DNS server (based on RFC 1877). Then, it forwards DNS queries from DHCP clients to this server and sends the response back to the DHCP clients. None - there is no second or third DNS server.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

9.3 Static DHCP Screen

Use this screen to assign static IP address to specific computers. To open this screen, click **Network > DHCP Server > Static DHCP**.

Figure 72 Network > DHCP Server > Static DHCP

The screenshot shows the 'Static DHCP' configuration screen. At the top, there are three tabs: 'General', 'Static DHCP' (which is selected), and 'Client List'. Below the tabs is the title 'Static DHCP Table'. The table has three columns: '#', 'MAC Address', and 'IP Address'. There are 8 rows, each with a number in the first column, an empty text box in the second column, and '0.0.0.0' in the third column. Below the table, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 56 DHCP Setup

LABEL	DESCRIPTION
#	This field is a sequential value.
MAC Address	Enter the MAC address of the computer to which you want to assign a static IP address.

Table 56 DHCP Setup

LABEL	DESCRIPTION
IP Address	Enter the static IP address you want to assign to the specified computer.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

9.4 Client List Screen

Use this screen to look at the current list of DHCP clients. It is empty if the DHCP server is disabled. To open this screen, click **Network > DHCP Server > Client List**.

Figure 73 Network > DHCP Server > Client List

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	tw11477-02	00:50:8d:48:59:1f	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 57 Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any entry.
IP Address	This field displays the IP address assigned to the computer.
Host Name	This field displays the host name of the computer.
MAC Address	This field displays the MAC address of the computer to which the IP address is assigned.
Reserve	Select this, and click Apply to use the information in this entry to create an entry in the Static DHCP table. See Network > DHCP Server > Static DHCP .
Apply	Click this to save your changes back to the ZyXEL Device.
Refresh	Click this to update this screen.

CHAPTER 10

NAT

Use these screens to configure port forwarding, trigger ports, and other NAT rules for the ZyXEL Device. See [Appendix D on page 381](#) for more background information about NAT.

10.1 NAT Overview

10.1.1 Port Forwarding: Services and Port Numbers

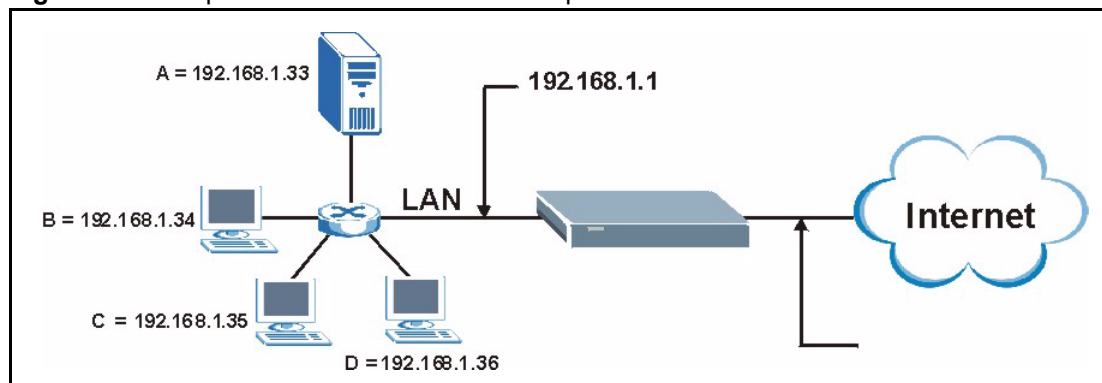
A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

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

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded. See [Appendix I on page 431](#) for examples of services.

For 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 74 Multiple Servers Behind NAT Example



10.1.2 Trigger Port Forwarding

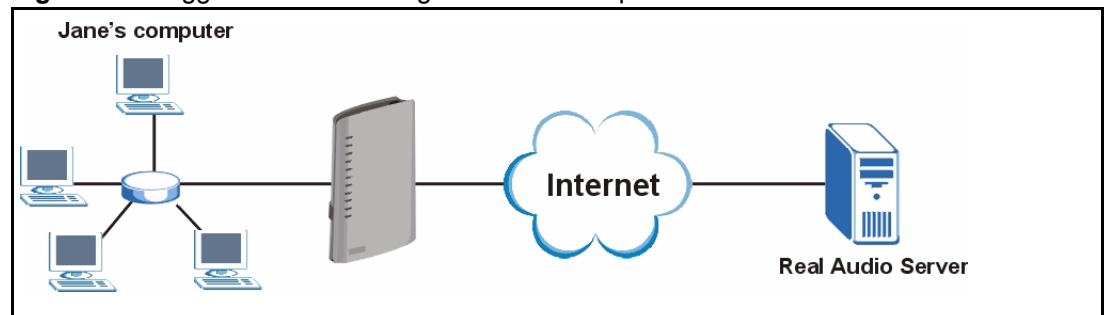
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem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

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

10.1.2.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 75 Trigger Port Forwarding Process: Example



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

10.1.2.2 Two Points To Remember About Trigger Ports

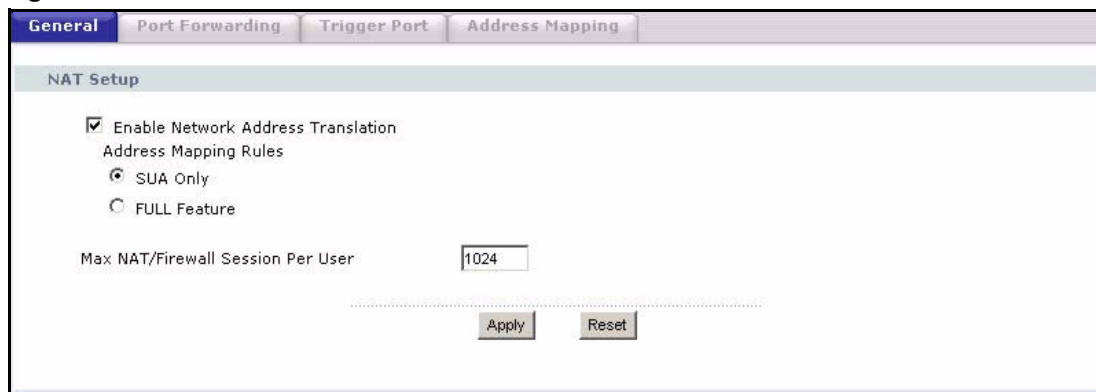
- 1 Trigger events only happen on data that is going coming from inside the ZyXEL Device and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

10.2 General NAT Screen

Use this screen to enable and disable port forwarding, trigger port, and other NAT rules. To open this screen, click **Network > NAT > General**.

Note: Make sure your firewall allows the traffic you specify in the NAT screens to be forwarded through the ZyXEL Device. You might have to create a firewall rule.

Figure 76 Network > NAT > General



The following table describes the labels in this screen.

Table 58 Network > NAT > General

LABEL	DESCRIPTION
Enable Network Address Translation	Select this to enable port forwarding, trigger ports, and NAT.
SUA Only	Select this if you have only one WAN IP address for your ZyXEL Device.
Full Feature	Select this if you have more than one public WAN IP address for your ZyXEL Device.
Max NAT/Firewall Session Per User	Select the maximum number of NAT rules and firewall rules the ZyXEL Device enforces at one time. The ZyXEL Device automatically allocates memory for the maximum number of rules, regardless of whether or not there is a rule to enforce.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

10.3 Port Forwarding Screen

Use this screen to look at the current port-forwarding rules in the ZyXEL Device, and to enable, disable, activate, and deactivate each one. You can also set up a default server to handle ports not covered by rules. To open this screen, click **Network > NAT > Port Forwarding**.

Figure 77 Network > NAT > Port Forwarding

#	Active	Name	Start Port	End Port	Server IP Address	Modify
1			0	0		
2			0	0		
3			0	0		
4			0	0		
5			0	0		
6			0	0		
7			0	0		
8			0	0		
9			0	0		
10			0	0		
11			0	0		

The following table describes the fields in this screen.

Table 59 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	Enter the IP address of the server to which the ZyXEL Device should forward packets for ports that are not specified in the Port Forwarding section below or in the Management > Remote MGMT screens. Enter 0.0.0.0 if you want the ZyXEL Device to discard these packets instead.
Port Forwarding	
#	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 active rule in order, and it only follows the first one that applies.
Active	Select this to enable this rule. Clear this to disable this rule.
Name	This field displays the name of the rule. It does not have to be unique.
Start Port	This field displays the beginning of the range of port numbers forwarded by this rule.
End Port	This field displays the end of the range of port numbers forwarded by this rule. If it is the same as the Start Port , only one port number is forwarded.

Table 59 Network > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Server IP Address	This field displays the IP address of the server to which packet for the selected port(s) are forwarded.
Modify	This column provides icons to edit and delete rules. To edit a rule, click the Edit icon next to the rule. The Port Forwarding Edit screen appears. To delete a rule, click the Remove icon next to the rule. All the information in the rule returns to the default settings.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

10.3.1 Port Forwarding Edit Screen

Use this screen to activate, deactivate, and edit each port-forwarding rule in the ZyXEL Device. To open this screen, click an **Edit** icon in **Network > NAT > Port Forwarding**.

Figure 78 Network > NAT > Port Forwarding > Edit

The following table describes the fields in this screen.

Table 60 Network > NAT > Port Forwarding > Edit

LABEL	DESCRIPTION
Active	Select this to enable this rule. Clear this to disable this rule.
Service Name	Enter a name to identify this rule. You can use 1 - 31 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Start Port End Port	Enter the port number or range of port numbers you want to forward to the specified server. To forward one port number, enter the port number in the Start Port and End Port fields. To forward a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start Port field enter the port number at the end of the range in the End Port field.
Server IP Address	Enter the IP address of the server to which to forward packets for the selected port number(s). This server is usually on the LAN.

Table 60 Network > NAT > Port Forwarding > Edit (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to return to the previous screen without saving any changes.

10.4 Trigger Port Screen

Use this screen to maintain port-triggering rules in the ZyXEL Device. To open this screen, click **Network > NAT > Trigger Port**.

Figure 79 Network > NAT > Trigger Port

Port Triggering Rules					
#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

The following table describes the fields in this screen.

Table 61 Network > NAT > Trigger Port

LABEL	DESCRIPTION
Name	Enter a name to identify this rule. You can use 1 - 15 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Incoming	

Table 61 Network > NAT > Trigger Port (continued)

LABEL	DESCRIPTION
Start Port End Port	Enter the incoming port number or range of port numbers you want to forward to the IP address the ZyXEL Device records. To forward one port number, enter the port number in the Start Port and End Port fields. To forward a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start Port field enter the port number at the end of the range in the End Port field. If you want to delete this rule, enter zero in the Start Port and End Port fields.
Trigger	
Start Port End Port	Enter the outgoing port number or range of port numbers that makes the ZyXEL Device record the source IP address and assign it to the selected incoming port number(s). To select one port number, enter the port number in the Start Port and End Port fields. To select a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start Port field enter the port number at the end of the range in the End Port field. If you want to delete this rule, enter zero in the Start Port and End Port fields.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

10.5 Address Mapping Screen

Use this screen to edit other NAT rules for your ZyXEL Device. To open this screen, click **Network > NAT > Address Mapping**.

Figure 80 Network > NAT > Address Mapping

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 62 Network > NAT > Address Mapping

LABEL	DESCRIPTION
#	This is the rule index number.
Local Start IP Local End IP	This is the range of IP addresses on the LAN port. Local Start IP is N/A for Server port mapping. Local End IP is N/A for One-to-one and Server mapping types.
Global Start IP Global End IP	This is the corresponding range of IP addresses on the WAN port. Global Start IP should be 0.0.0.0 if both of the following conditions are satisfied. <ul style="list-style-type: none"> Your ISP assigns the IP address of your WAN port. The rule is a Many-to-One or Server rule. Global End IP is N/A for One-to-one , Many-to-One and Server mapping types.
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	This column provides icons to edit and delete rules. To edit a rule, click the Edit icon next to the rule. The Address Mapping Edit screen appears. To delete a rule, click the Remove icon next to the rule. All the information in the rule returns to the default settings.

10.5.1 Address Mapping Edit Screen

Use this screen to activate, deactivate, and edit each address mapping rule in the ZyXEL Device. To open this screen, click an **Edit** icon in **Network > NAT > Address Mapping**.

Figure 81 Network > NAT > Address Mapping > Edit

The screenshot shows the 'Edit Address Mapping Rule 1' interface. It contains the following fields and controls:

- Type**: A dropdown menu set to 'One-to-One'.
- Local Start IP**: A text input field containing '0.0.0.0'.
- Local End IP**: A text input field containing 'N/A'.
- Global Start IP**: A text input field containing '0.0.0.0'.
- Global End IP**: A text input field containing 'N/A'.
- At the bottom, there are three buttons: '<Back', 'Apply', and 'Cancel'.

The following table describes the fields in this screen.

Table 63 Network > NAT > Address Mapping > Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <ul style="list-style-type: none"> • 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. • 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. • Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. • Many-to-Many No Overload: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. • Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP Local End IP	Enter the range of IP addresses on the LAN port. Local Start IP is N/A for Server port mapping. Local End IP is N/A for One-to-one and Server mapping types. To create a rule for all LAN IP addresses, set Local Start IP to 0.0.0.0 and Local End IP to 255.255.255.255.
Global Start IP Global End IP	This is the corresponding range of IP addresses on the WAN port. Global Start IP should be 0.0.0.0 if both of the following conditions are satisfied. <ul style="list-style-type: none"> • Your ISP assigns the IP address of your WAN port. • The rule is a Many-to-One or Server rule. Global End IP is N/A for One-to-one , Many-to-One and Server mapping types.
Back	Click this to return to the previous screen without saving any changes.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

CHAPTER 11

Firewalls

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

11.1 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.

11.1.1 Stateful Inspection Firewalls

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

11.1.2 About the ZyXEL Device Firewall

The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. 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 port and four Ethernet LAN ports, which physically separate the network into two areas.

- The DSL port connects to the Internet.
- The LAN (Local Area Network) ports attach 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.

11.1.3 Firewall Rule Direction

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.

11.1.4 Firewall Rule Logic

Note: Study these points carefully before configuring rules.

11.1.4.1 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.

11.1.4.2 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.

11.1.5 Firewall Rule Services

Most programs use services to communicate across the Internet. Many of these services are already defined in the ZyXEL Device, and you can set up additional ones, if necessary.

In general, services are consist of two parts. First, each service has one or two IP protocol types (for example, TCP, UDP, or TCP/UDP). Second, each service has one or more port numbers. Together, these parts define the service. See [Appendix I on page 431](#) for examples of services.

11.1.6 DoS Thresholds

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

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

11.1.6.1 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.

11.1.6.2 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. 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.

11.1.6.3 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:

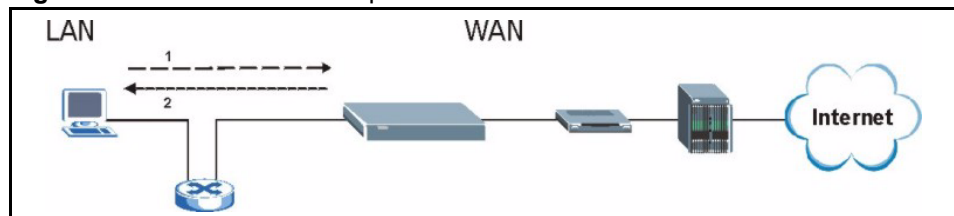
- If the **Blocking Time** timeout is 0 (the default), then the ZyXEL Device deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking 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.

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.

11.2 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 82 Ideal Firewall Setup



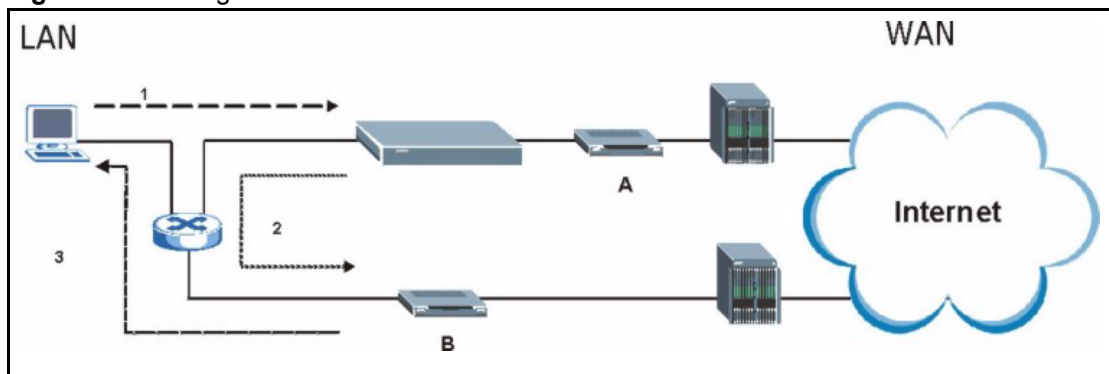
11.2.1 The “Triangle Route” Problem

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 83 “Triangle Route” Problem



11.2.2 Solving the “Triangle Route” Problem

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

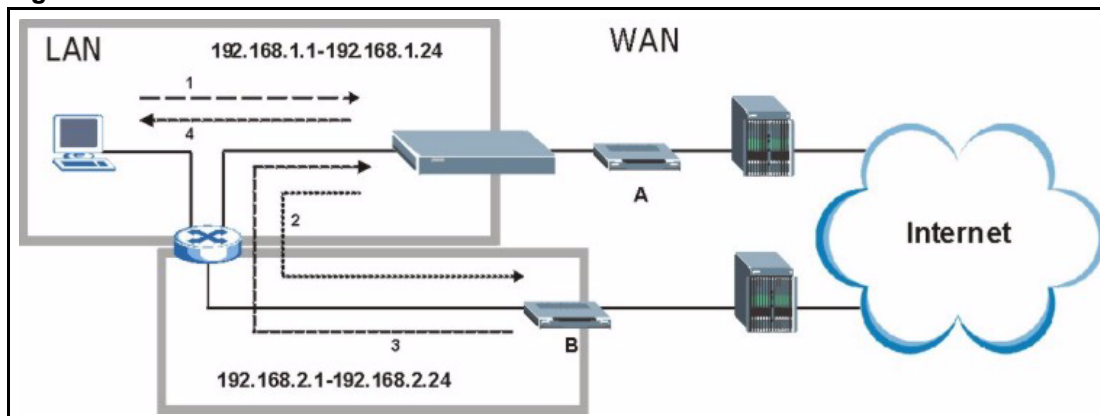
Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyXEL Device supports up to three logical LAN interfaces with the ZyXEL Device being the gateway for each logical network.

It's like having multiple LAN networks that actually use the same physical cables and ports. 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 84 IP Alias



11.3 Guidelines for Enhancing Security with Your Firewall

- Change the default password via CLI (Command Line Interpreter) or web configurator.
- 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.

11.3.1 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.

11.4 General Firewall Screen

Use this screen to activate the firewall and to set the default rules for each direction. To open this screen, click **Security > Firewall > General**.

Figure 85 Security > Firewall > General

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

The following table describes the labels in this screen.

Table 64 Security > Firewall > General

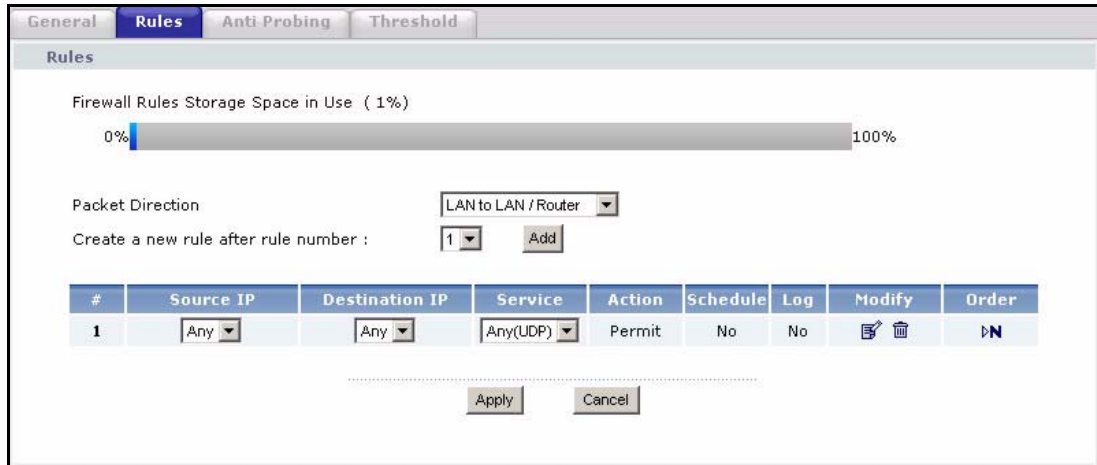
LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the ZyXEL Device firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology. Note: Allowing asymmetrical routes may let traffic from the WAN go directly to a LAN computer without passing through the router.
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 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.
Expand...	Click this button to display more information.
Basic...	Click this button to display less information.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

11.5 Firewall Rules Screen

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

Use this screen to activate the firewall and to set the default rules for each direction. To open this screen, click **Security > Firewall > Rules**.

Figure 86 Security > Firewall > Rules



The following table describes the labels in this screen.

Table 65 Security > Firewall > Rules

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyXEL Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click Add to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
	The following fields summarize the rules you have created that apply to traffic traveling in the selected Packet Direction . These rules take priority over the general firewall action settings in the Security > Firewall > General screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in order.
Active	This field displays whether a firewall is turned on or not. Select this to enable the rule. Clear this 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).

Table 65 Security > Firewall > Rules (continued)

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

11.5.1 Firewall Rule Edit Screen

Use this screen to create a new firewall rule or to edit an existing one. To open this screen, click **Add** or click an **Edit** icon in **Security > Firewall > Rules**.

Figure 87 Security > Firewall > Rules > Edit

Edit Rule 1

Active
 Action for Matched Packets: Permit

Source Address

Address Type: Any Address Source Address List

Start IP Address: 0.0.0.0 Add >>

End IP Address: 0.0.0.0 Edit <<

Subnet Mask: 0.0.0.0 Delete

Destination Address

Address Type: Any Address Destination Address List

Start IP Address: 0.0.0.0 Add >>

End IP Address: 0.0.0.0 Edit <<

Subnet Mask: 0.0.0.0 Delete

Service

Available Services:
 Any(All)
 Any(ICMP)
 AIMNEW_ICQ(TCP:5190)
 AUTH(TCP:113)
 BGP(TCP:179)
 Add >>

Remove

[Edit Customized Services](#)

Selected Services:
 Any(UDP)
 Any(TCP)

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 66 Security > Firewall > Rules > Edit

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select Drop to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select Reject to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select Permit to allow the passage of the packets.
Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: Single Address , Range Address , Subnet Address and Any Address .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click Add >> to add a new address to the Source or Destination Address box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click Edit << .
Delete	Highlight an existing source or destination address from the Source or Destination Address box above and click Delete to remove it.
Services	
Available / Selected Services	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.

Table 66 Security > Firewall > Rules > Edit (continued)

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

11.5.2 Customized Services Screen

Use this screen to create or edit customized services for firewall rules. Customized services and port numbers are not predefined by the ZyXEL Device. See [Appendix I on page 431](#) for examples of services. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website.

To open this screen, click **Edit Customized Services** in **Security > Firewall > Rules > Edit**.

Figure 88 Security > Firewall > Rules > Edit > Edit Customized Services

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

.....
<Back

The following table describes the labels in this screen.

Table 67 Security > Firewall > Rules > Edit > Edit Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to a screen where you can 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 this to return the previous screen.

11.5.3 Customized Service Edit Screen

Use this screen to create or edit a customized service for firewall rules. To open this screen, click a rules number in **Security > Firewall > Rules > Edit > Edit Customized Services**.

Figure 89 Security > Firewall > Rules > Edit > Edit Customized Services > Edit

The following table describes the labels in this screen.

Table 68 Security > Firewall > Rules > Edit > Edit Customized Services > Edit

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

11.6 Anti-Probing Screen

Use this screen to control the way the ZyXEL Device responds to ping requests and to requests for unsupported services. Normally, if an outside user attempts to probe an unsupported port on your ZyXEL Device, the ZyXEL Device sends a response. This allows the outside user to know the ZyXEL Device exists. The ZyXEL Device supports anti-probing, which prevents the ZyXEL Device from sending the response. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

To open this screen, click a rules number in **Security > Firewall > Anti Probing**.

Figure 90 Security > Firewall > Anti Probing

The following table describes the labels in this screen.

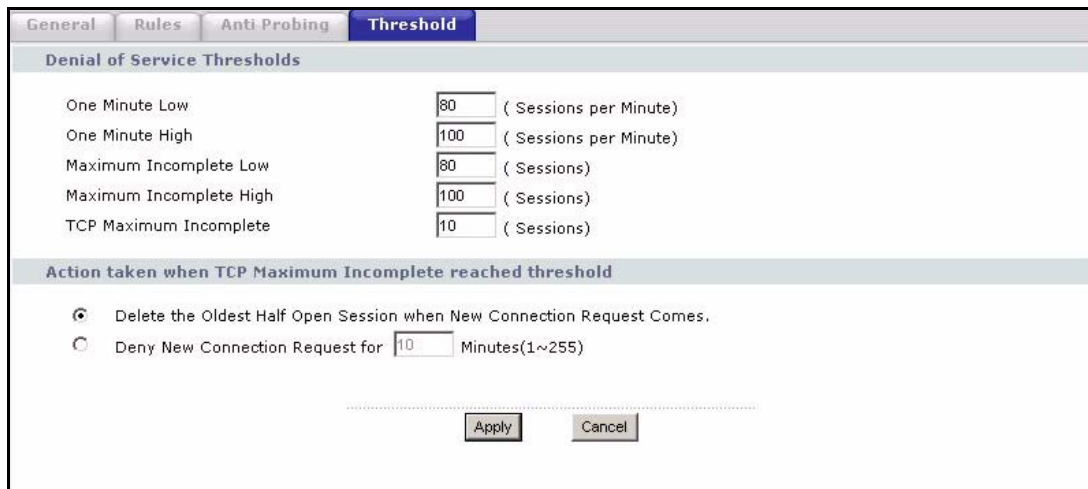
Table 69 Security > Firewall > Anti Probing

LABEL	DESCRIPTION
Respond to PING on	The ZyXEL Device does 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 changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

11.7 Firewall Threshold Screen

Use this screen to set various DoS thresholds and the maximum number of half-open sessions. To open this screen, click a rules number in **Security > Firewall > Threshold**.

Figure 91 Security > Firewall > Threshold



The following table describes the labels in this screen.

Table 70 Security > 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.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection attempts.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set Maximum Incomplete High to lower than the current Maximum Incomplete Low number.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.
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.

Table 70 Security > Firewall > Threshold (continued)

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

CHAPTER 12

Content Filter

Use these screens to create and enforce policies that restrict access to the Internet based on content.

12.1 Content Filtering Overview

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

The ZyXEL Device can block web features such as ActiveX controls, Java applets, cookies and disable web proxies. The ZyXEL Device also allows you to define time periods and days during which the ZyXEL Device performs content filtering.

12.2 Content Filtering Screens

12.2.1 Content Filter Screen

Use this screen to set up a trusted IP address, which web features are restricted, and which keywords are blocked when content filtering is effective. To access this screen, click **Security > Content Filter > Filter**.

Figure 92 Security > Content Filter > Filter

Each field is described in the following table.

Table 71 Security > Content Filter > Filter

LABEL	DESCRIPTION
Trusted IP Setup	
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without the restrictions you set in these screens. Enter the IP address of the trusted computer. Enter 0.0.0.0 if no computer should have access to Internet resources without restrictions.
Restrict Web Features	<p>Select the web features you want to disable. If a user downloads a page with a restricted feature, that part of the web page appears blank or grayed out.</p> <p>ActiveX - This is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.</p> <p>Java - This is used to build downloadable Web components or Internet and intranet business applications of all kinds.</p> <p>Cookies - This is used by Web servers to track usage and to provide service based on ID.</p> <p>Web Proxy - This is a server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN, it is possible for LAN users to avoid content filtering restrictions.</p>
Keyword Blocking	
Enable URL Keyword Blocking	Select this if you want the ZyXEL Device to block Web sites based on words in the web site address. For example, if you block the keyword bad , http://www.website.com/bad.html is blocked.

Table 71 Security > Content Filter > Filter

LABEL	DESCRIPTION
Keyword	Type a keyword you want to block in this field. You can use up to 64 printable ASCII characters. There is no wildcard character, however.
Add	Click this to add the specified Keyword to the Keyword List . You can enter up to 64 keywords.
Keyword List	This field displays the keywords that are blocked when Enable URL Keyword Blocking is selected. To delete a keyword, select it, click Delete , and click Apply .
Delete	Click Delete to remove the selected keyword in the Keyword List . The keyword disappears after you click Apply .
Clear All	Click this button to remove all of the keywords in the Keyword List .
Denied Access Message	Enter the message that is displayed when the ZyXEL Device's content filter feature blocks access to a web site.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

12.2.2 Content Filter Schedule Screen

Use this screen to set up the schedule when content filtering is effective. To access this screen, click **Security > Content Filter > Schedule**.

Figure 93 Security > Content Filter > Schedule

Each field is described in the following table.

Table 72 Security > Content Filter > Schedule

LABEL	DESCRIPTION
Day to Block	Select which days of the week you want content filtering to be effective.
Time of Day to Block	Select what time each day you want content filtering to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

CHAPTER 13

Certificates

This chapter explains how to use certificates with your ZyXEL Device.

13.1 Certificates Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users and to let users authenticate the ZyXEL Device. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

13.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

13.1.2 Self-signed Certificates

You can have the ZyXEL Device act as a certification authority and sign its own certificates.

13.1.3 Certificate File Formats

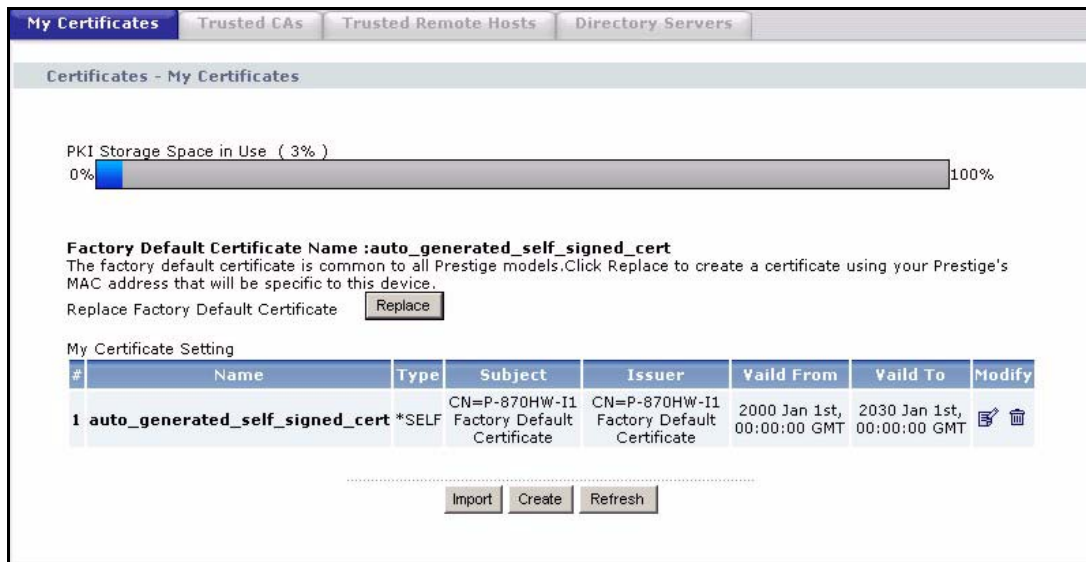
The ZyXEL Device supports the following formats for certification authority certificates.

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKCS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

13.2 My Certificates Screen

Use this screen to look at the ZyXEL Device's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. To open this screen, click **Security > Certificates > My Certificates**.

Figure 94 Security > Certificates > My Certificates



The following table describes the labels in this screen.

Table 73 Security > Certificates > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyXEL Device has the factory default certificate. The factory default certificate is common to all ZyXEL Device that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyXEL Device's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request. SELF represents a self-signed certificate. *SELF represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates. CERT represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.

Table 73 Security > Certificates > My Certificates (continued)

LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	<p>Click an Edit icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click a Remove icon to remove the certificate. You cannot delete a certificate that is used by any features.</p> <p>Do the following to delete the certificate that shows *SELF in the Type field.</p> <ol style="list-style-type: none"> 1. Make sure that no other features, such as remote management, are configured to use the *SELF certificate. 2. Click the Edit icon next to another self-signed certificate. 3. Select the Default self-signed certificate which signs the imported remote host certificates. check box. 4. Click Apply to save the changes and return to the My Certificates screen. 5. The certificate that originally showed *SELF displays SELF and you can delete it now. <p>Note that subsequent certificates move up by one when you take this action</p>
Import	Click this to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.
Create	Click this to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.
Refresh	Click this to update the screen.

13.3 Import My Certificate Screen

Use this screen to save an existing certificate to the ZyXEL Device. To open this screen, click **Import** in **Security > Certificates > My Certificates**.

Note: You can only import a certificate that matches a corresponding certification request that was generated by the ZyXEL Device. In addition, the certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 95 Security > Certificates > My Certificates > Import

CERTIFICATES - MY CERTIFICATE - IMPORT

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on Prestige. After the importation, the certification request will automatically be deleted.

File Path:

The following table describes the labels in this screen.

Table 74 Security > Certificates > My Certificates > Import

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 this to find the certificate file you want to upload.
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to return to the previous screen without saving any changes.

13.4 Create My Certificate Screen

Use this screen to have the ZyXEL Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request. To open this screen, click **Create** in **Security > Certificates > My Certificates**.

Figure 96 Security > Certificates > My Certificates > Create

The following table describes the labels in this screen.

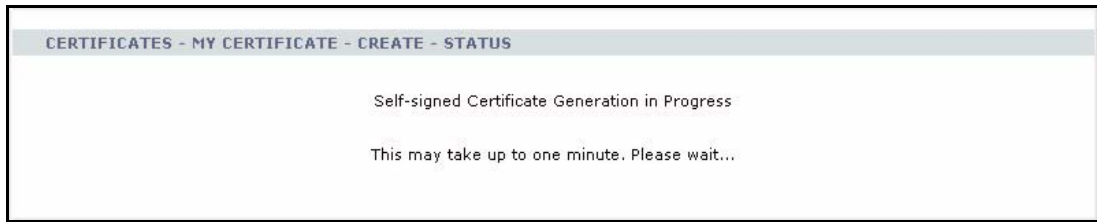
Table 75 Security > Certificates > My Certificates > Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the Common Name is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.

Table 75 Security > Certificates > My Certificates > Create (continued)

LABEL	DESCRIPTION
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select this to have the ZyXEL Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the ZyXEL Device generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the Edit My Certificate screen and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select this to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the Trusted CAs screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the Reference Number and Key if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. Certificate Management Protocol (CMP) is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the CA Certificate drop-down list box. You must have the certification authority's certificate already imported in the Trusted CAs screen. Click Trusted CAs to go to the Trusted CAs screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication Request Number	When you select Create a certification request and enroll for a certificate immediately online , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just fill in the Key field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.
Export	Click this to save the certificate on your computer.
Apply	Click this to begin certificate or certification request generation.
Cancel	Click this to return to the previous screen without saving any changes.

After you click **Apply**, the following screen appears.

Figure 97 Security > Certificates > My Certificates > Create > In Progress

Wait while the ZyXEL Device generates the self-signed certificate or certification request. Afterwards, the following screen should appear.

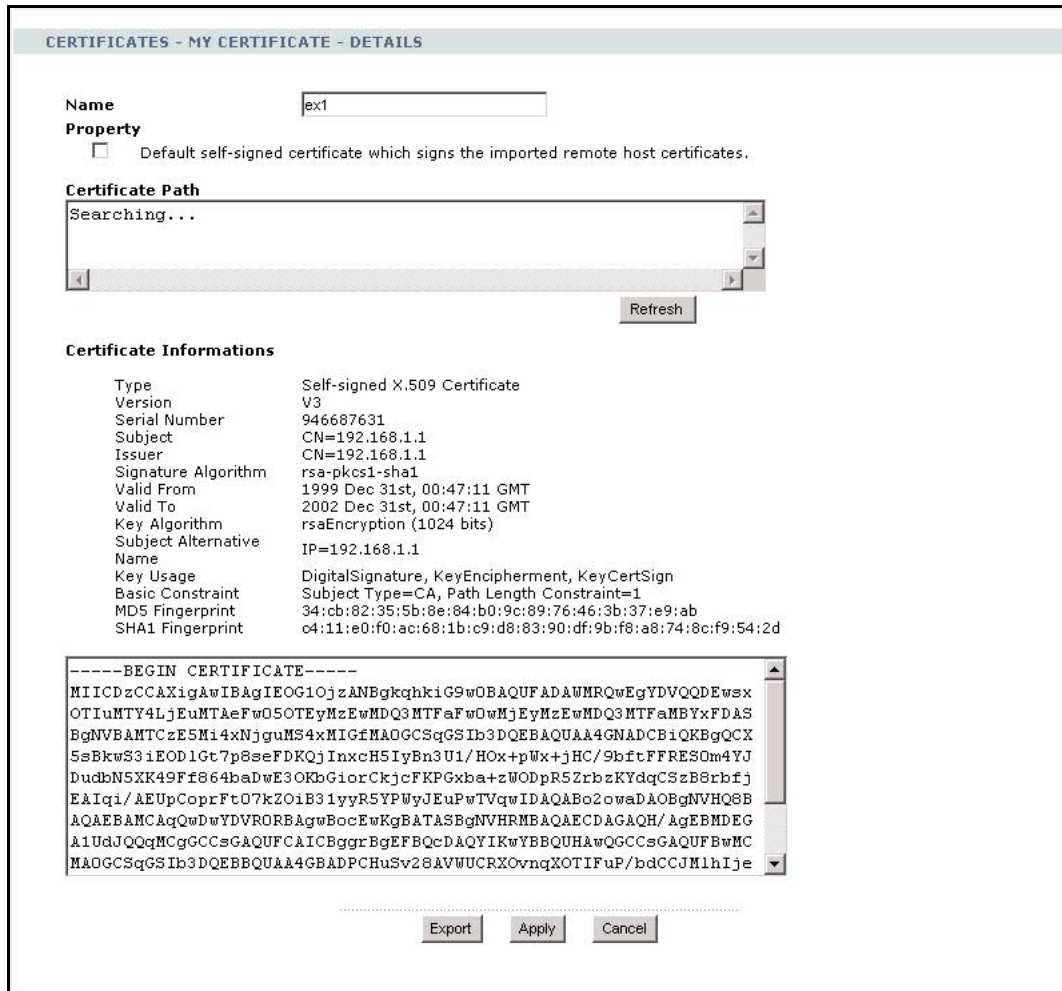
Figure 98 Security > Certificates > My Certificates > Create > Successful

If the ZyXEL Device is successful, click **Return** to go to the **Security > Certificates > My Certificates** screen. Otherwise, click **Return** to go to the **Security > Certificates > My Certificates > Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyXEL Device to enroll a certificate online.

13.5 Edit My Certificates Screen

Use this screen to view in-depth certificate information or change the certificate's name. To open this screen, click an **Edit** icon in **Security > Certificates > My Certificates**.

Figure 99 Security > Certificates > My Certificates > Edit



The following table describes the labels in this screen.

Table 76 Security > Certificates > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property	
Default self-signed certificate which signs the imported remote host certificates.	Select this if you want to make this self-signed certificate the default certificate.
Certificate Path	This field displays the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate in the path has expired or been revoked.

Table 76 Security > Certificates > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Refresh	Click this to display the certification path.
Certificate Informations	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyXEL Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm.

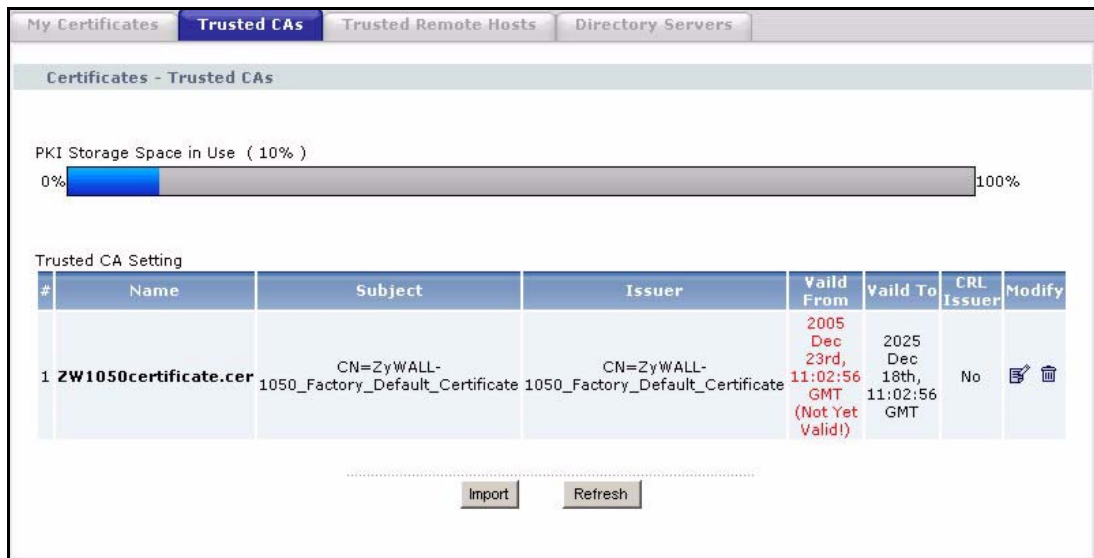
Table 76 Security > Certificates > My Certificates > Edit (continued)

LABEL	DESCRIPTION
-- BEGIN CERTIFICATE --	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Export	Click this to save the certificate on your computer.
Apply	Click this to save your changes to the ZyXEL Device.
Cancel	Click this to return to the previous screen without saving any changes.

13.6 Trusted CAs Screen

Use this screen to look at certificates from certification authorities that the ZyXEL Device trusts. The ZyXEL Device accepts any valid certificate signed by these certification authorities as being trustworthy so that you do not need to import such certificates. To open this screen, click **Security > Certificates > Trusted CAs**.

Figure 100 Security > Certificates > Trusted CAs



The following table describes the labels in this screen.

Table 77 Security > Certificates > Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the Issues certificate revocation lists (CRL) check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Modify	Click an Edit icon to open a screen with an in-depth list of information about the certificate. Click a Remove icon to remove the certificate.

Table 77 Security > Certificates > Trusted CAs (continued)

LABEL	DESCRIPTION
Import	Click this to open the Import Trusted CA screen.
Refresh	Click this to update the screen.

13.7 Import Trusted CA Screen

Use this screen to add the certificate of a trusted certification authority to the ZyXEL Device. To open this screen, click **Import** in **Security > Certificates > Trusted CAs**.

Note: You must remove any spaces in the certificate's file name before you import the certificate.

Figure 101 Security > Certificates > Trusted CAs > Import

The following table describes the labels in this screen.

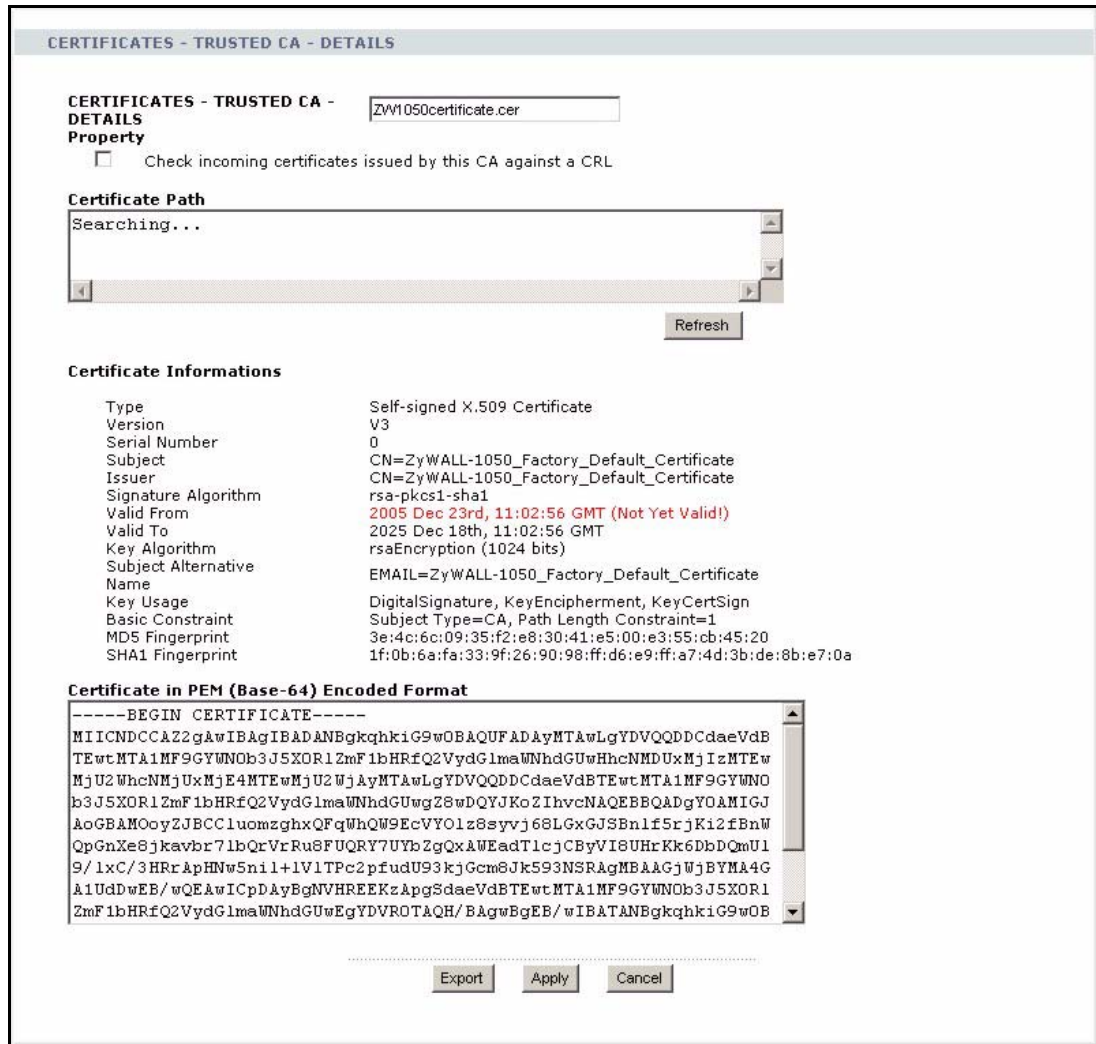
Table 78 Security > Certificates > Trusted CAs > Import

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 this to find the certificate file you want to upload.
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to return to the previous screen without saving any changes.

13.8 Edit Trusted CA Screen

Use this screen to view in-depth information about the certification authority's certificate or change the certificate's name. In addition, you can also specify whether or not to check certificates from the certification authority against a list of revoked certificates. To open this screen, click an **Edit** icon in **Security > Certificates > Trusted CAs**.

Figure 102 Security > Certificates > Trusted CAs > Edit



The following table describes the labels in this screen.

Table 79 Security > Certificates > Trusted CAs > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Check incoming certificates issued by this CA against a CRL	Select this to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certification Path	This field displays the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.

Table 79 Security > Certificates > Trusted CAs > Edit (continued)

LABEL	DESCRIPTION
Refresh	Click this to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You can use this value to verify that this is the remote host's actual certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You can use this value to verify that this is the remote host's actual certificate.

Table 79 Security > Certificates > Trusted CAs > Edit (continued)

LABEL	DESCRIPTION
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this to save the certificate on your computer.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to return to the previous screen without saving any changes.

13.9 Trusted Remote Hosts Screen

Use this screen to look at the certificates of peers that you trust but which are not signed by one of the trusted certification authorities (on the **Security > Certificates > Trusted CAs** screen). To open this screen, click **Security > Certificates > Trusted Remote Hosts**.

You do not need to add any certificate that is signed by one of the trusted certification authorities on the **Trusted CAs** screen since the ZyXEL Device automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

Figure 103 Security > Certificates > Trusted Remote Hosts



The following table describes the labels in this screen.

Table 80 Security > Certificates > Trusted Remote Hosts

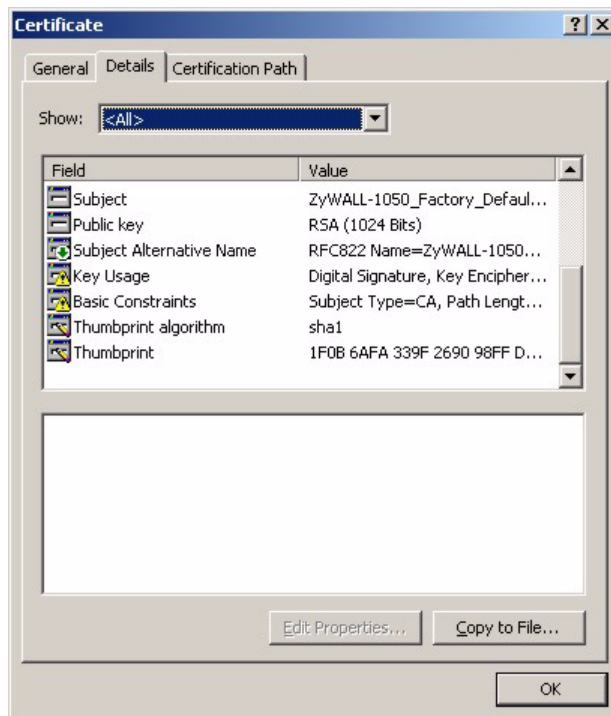
LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click an Edit icon to open the Edit Trusted Remote Host screen. Click a Remove icon to remove the certificate.
Import	Click this to open the Import Trusted Remote Host screen.
Refresh	Click this to update this screen.

13.10 Verifying a Trusted Remote Host's Certificate

Self-signed certificates only have the signature of the host itself. You should be very careful about importing (and thereby trusting) a remote host's self-signed certificate. You can follow these steps to check that you have the remote host's actual certificate.

- 1 Open Windows Explorer.
- 2 Find the certificate, and double-click on it. The **Certificate** window appears.
- 3 Click the **Details** tab.
- 4 Scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 104 Certificate Details



Verify (over the phone, for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

13.11 Import Trusted Remote Host Screen

Before you import a certificate, see [Section 13.10 on page 186](#).

Use this screen to add the certificate of a trusted host to the ZyXEL Device. To open this screen, click **Import** in **Security > Certificates > Trusted Remote Hosts**.

Note: The trusted remote host certificate must be a self-signed certificate, and you must remove any spaces from its file name before you can import it.

Figure 105 Security > Certificates > Trusted Remote Host > Import

CERTIFICATES - TRUSTED REMOTE HOST - IMPORT

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path:

The following table describes the labels in this screen.

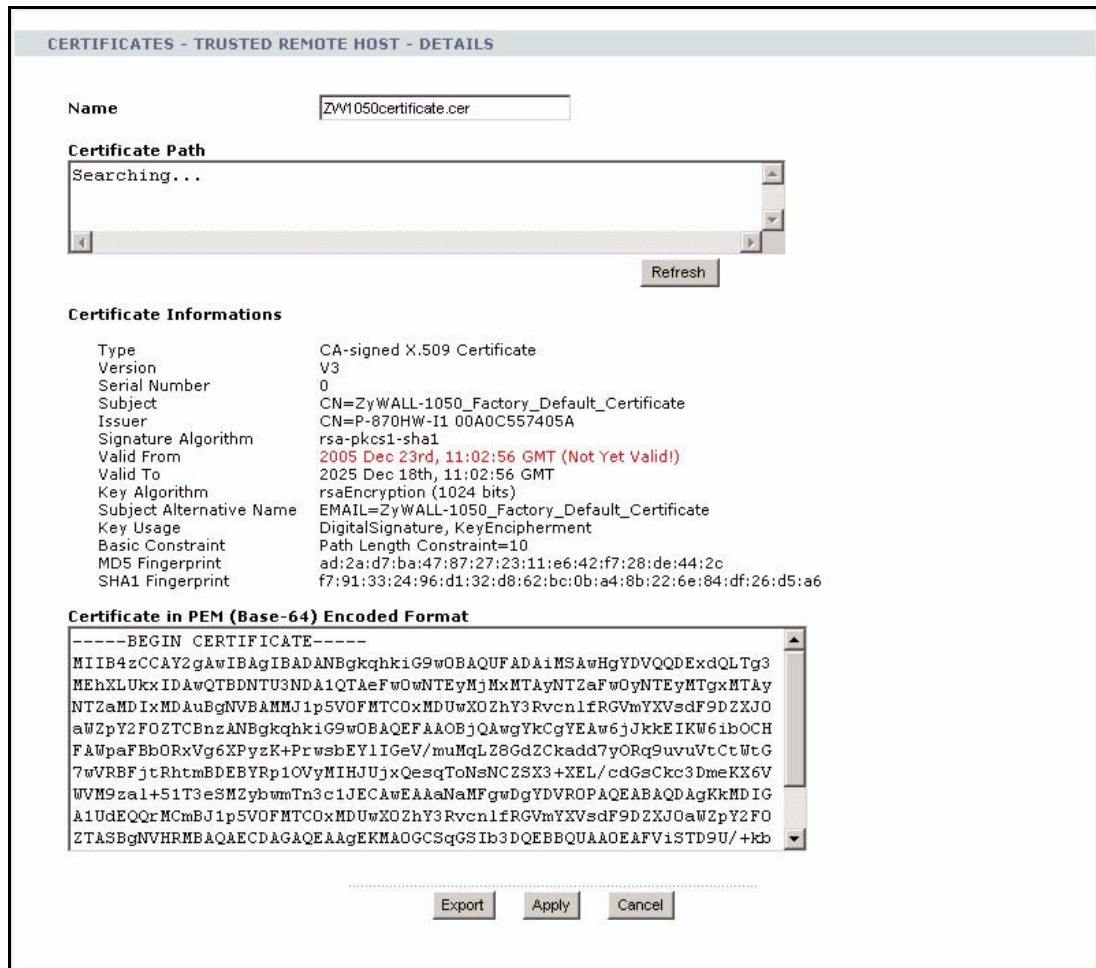
Table 81 Security > Certificates > Trusted Remote Host > Import

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 this to find the certificate file you want to upload.
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to return to the previous screen without saving any changes.

13.12 Edit Trusted Remote Host Screen

Use this screen to view in-depth information about the trusted remote host's certificate or change the certificate's name. To open this screen, click an **Edit** icon in **Security > Certificates > Trusted Remote Hosts**.

Figure 106 Security > Certificates > Trusted Remote Hosts > Edit



The following table describes the labels in this screen.

Table 82 Security > Certificates > Trusted Remote Hosts > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click Refresh to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyXEL Device uses to sign remote host certificates.
Refresh	Click this to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyXEL Device is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.

Table 82 Security > Certificates > Trusted Remote Hosts > Edit (continued)

LABEL	DESCRIPTION
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the ZyXEL Device used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 13.10 on page 186 for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 13.10 on page 186 for how to verify a remote host's certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this to save the certificate on your computer.

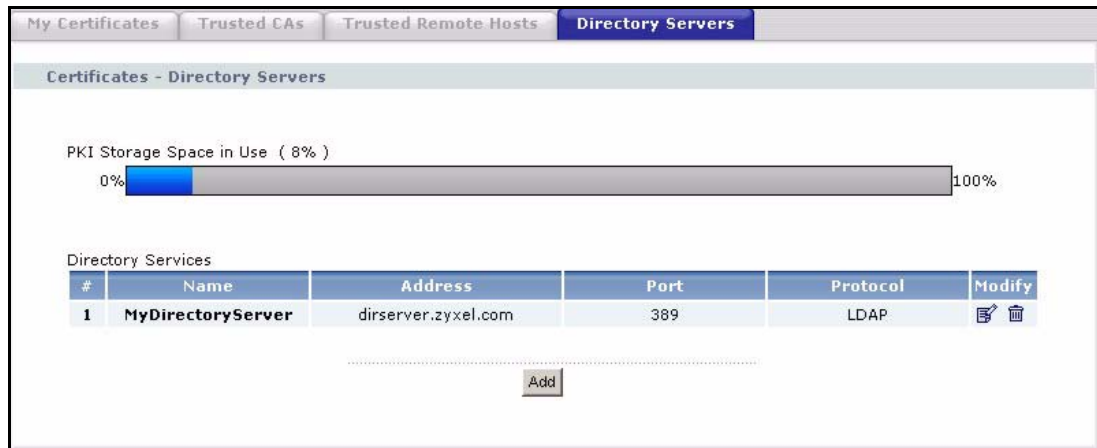
Table 82 Security > Certificates > Trusted Remote Hosts > Edit (continued)

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

13.13 Directory Servers Screen

Use this screen to look at the current list of directory servers, which the ZyXEL Device checks if the certificate does not list a server or if the listed server is not available. To open this screen, click **Security > Certificates > Directory Servers**.

Figure 107 Security > Certificates > Directory Servers



The following table describes the labels in this screen.

Table 83 Security > Certificates > Directory Servers

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click an Edit icon to open the Edit Directory Server screen. Click a Remove icon to remove the directory server entry.
Add	Click this to open the Edit Directory Server screen to add a new directory server.

13.14 Edit Directory Server Screen

Use this screen to create or edit a directory server the ZyXEL Device should use if the certificate does not list a server or if the listed server is not available. To open this screen, click **Add** or an **Edit** icon in **Security > Certificates > Directory Servers**.

Figure 108 Security > Certificates > Directory Servers > Edit

The following table describes the labels in this screen.

Table 84 Security > Certificates > Directory Servers > Edit

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol ^a	Use the drop-down list box to select the access protocol used by the directory server. LDAP (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.
Server Port	This field displays the default server port number of the protocol that you select in the Access Protocol field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The ZyXEL Device may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).

Table 84 Security > Certificates > Directory Servers > Edit (continued)

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

- a. At the time of writing, LDAP is the only choice of directory server access protocol.

CHAPTER 14

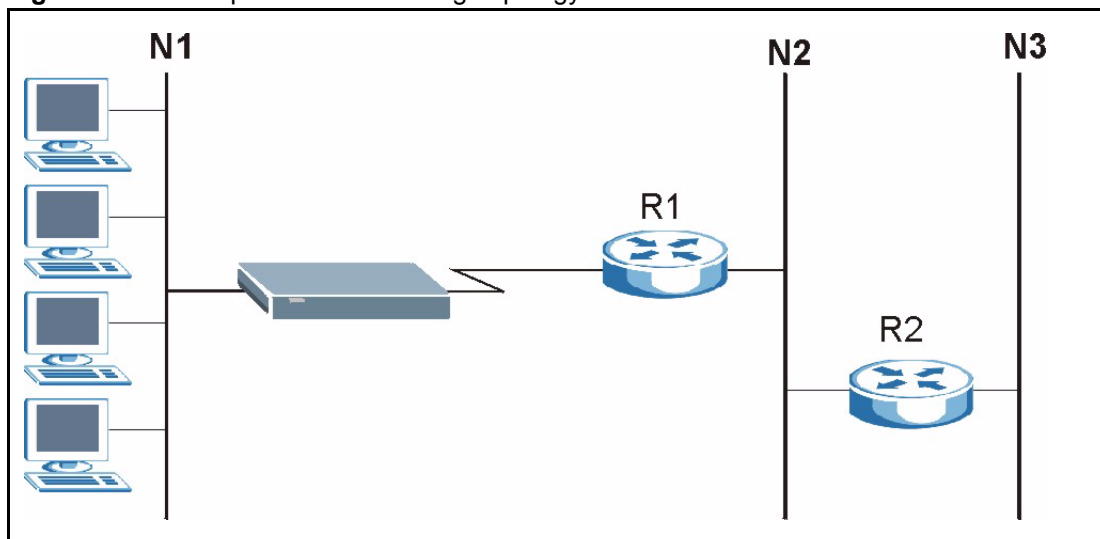
Static Route

Use these screens to configure static routes in the ZyXEL Device.

14.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 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 109 Example of Static Routing Topology



14.2 IP Static Route Screen

Use this screen to look at static routes in the ZyXEL Device. To open this screen, click **Management > Static Route > IP Static Route**.

Note: The first static route is the default route and cannot be modified or deleted.

Figure 110 Management > Static Route > IP Static Route

The screenshot shows the 'IP Static Route' configuration page. At the top, there is a header 'IP Static Route' and a sub-header 'Static Route Rules'. Below this is a table with the following columns: '#', 'Name', 'Active', 'Destination', 'Gateway', and 'Modify'. The table contains several rows, with the first three rows (1, 2, 3) and the last three rows (48, 49, 50) visible. Each row has a 'Modify' column containing an edit icon and a delete icon. The table is partially obscured by a wavy line, suggesting it is a scrollable list.

#	Name	Active	Destination	Gateway	Modify
1	-	-	
2	-	-	
3	-	-	
...
48	-	-	
49	-	-	
50	-	-	

Each field is described in the following table.

Table 85 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
#	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.
Name	This field displays the name that describes the static route.
Active	This field shows whether this static route is active (Yes) or not (No).
Destination	This field displays the destination IP address(es) that this static route affects.
Gateway	This field displays the IP address of the gateway to which the ZyXEL Device should send packets for the specified Destination . The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Use this field to edit or erase the static route. Click the Edit icon to open the Edit IP Static Route screen. Click the Remove icon to erase this static route.

14.2.1 Edit IP Static Route Screen

Use this screen to edit a static route in the ZyXEL Device. To access this screen, click an **Edit** icon in **Management > Static Route > IP Static Route**.

Figure 111 Management > Static Route > IP Static Route > Edit

Each field is described in the following table.

Table 86 Management > Static Route > IP Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the static route.
Active	Select this if you want the static route to be used. Clear this if you do not want the static route to be used.
Private	Select this if you do not want the ZyXEL Device to tell other routers about this static route. For example, you might select this if the static route is in your LAN. Clear this if you want the ZyXEL Device to tell other routers about this static route.
Destination IP Address	Enter one of the destination IP addresses that this static route affects.
IP Subnet Mask	Enter the subnet mask that defines the range of destination IP addresses that this static route affects. If this static route affects only one IP address, enter 255.255.255.255.
Gateway IP Address	Enter the IP address of the gateway to which the ZyXEL Device should send packets for the specified Destination . The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	This field is related to RIP. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the metric, the lower the "cost". RIP uses hop count as the measurement of cost, where 1 is for a directly-connected network. The metric must be 1-15; if you use a value higher than 15, the routers assume the link is down. Usually, you should keep the default value.
Apply	Click this to save your changes to the ZyXEL Device.
Cancel	Click this to return to the previous screen without saving your changes.

CHAPTER 15

Bandwidth MGMT

This chapter explains how to configure bandwidth management in your ZyXEL Device.

15.1 Bandwidth Management Overview

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

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

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

15.1.1 Priority-based Scheduler

Your ZyXEL Device uses a priority-based scheduler. A priority-based scheduler forwards traffic for applications (up to a limit you can specify for each application) according to the priorities that you assign to each application. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation. If two classes have the same priority, the ZyXEL Device divides bandwidth equally among bandwidth classes.

15.1.2 Bandwidth Management Priorities

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

Table 87 Bandwidth Management Priorities

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

15.1.3 Example: Unused and Unbudgeted Bandwidth

The following table shows the priorities of applications and the amount of bandwidth that each application gets.

Table 88 Example: Priority-based Allotment of Unused and Unbudgeted Bandwidth

BANDWIDTH CLASSES, PRIORITIES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: Low Priority, 1024 kbps
	Sales: High Priority, 3584 kbps
	Marketing: High Priority, 3584 kbps
	Research: Medium Priority, 2048 kbps

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

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

15.1.4 Reserving Bandwidth for Other Applications

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

- 1** Leave some of the interface's bandwidth unbudgeted.
- 2** Do not enable **Use All Managed Bandwidth** in the bandwidth filters.

15.1.5 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 89 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)	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.

15.2 Bandwidth Management Configuration Screen

Use this screen to enable bandwidth management and set the maximum allowed bandwidth for the **WAN** port. You can also set some basic settings for each rule. To open this screen, click **Management > Bandwidth MGMT > Configuration**.

Figure 112 Management > Bandwidth MGMT > Configuration

Configuration
Monitor

Bandwidth Management Setup

Active

LAN BW Budget(kbps):

WLAN BW Budget(kbps):

WAN BW Budget(kbps):

#	Direction	Name	Service	Dest Port	Priority	Modify
1	To LAN	LAN-VoIP (SIP)	VoIP(SIP)	0	High	
2	To LAN	LAN-WWW	User defined	0	Mid	
3	To WAN	WAN-VoIP (SIP)	VoIP(SIP)	0	High	
4	To WLAN	WLAN-VoIP (SIP)	VoIP(SIP)	0	High	
5	To WLAN	WLAN-WWW	User defined	0	Mid	
6	To LAN		User defined	0	High	
7	To LAN		User defined	0	High	
8	To LAN		User defined	0	High	
9	To LAN		User defined	0	High	
10	To LAN		User defined	0	High	
11	To LAN		User defined	0	High	
12	To LAN		User defined	0	High	
13	To LAN		User defined	0	High	
14	To LAN		User defined	0	High	
15	To LAN		User defined	0	High	
16	To LAN		User defined	0	High	
17	To LAN		User defined	0	High	
18	To LAN		User defined	0	High	
19	To LAN		User defined	0	High	
20	To LAN		User defined	0	High	
21	To LAN		User defined	0	High	
22	To LAN		User defined	0	High	
23	To LAN		User defined	0	High	
24	To LAN		User defined	0	High	
25	To LAN		User defined	0	High	
26	To LAN		User defined	0	High	
27	To LAN		User defined	0	High	

Apply
Reset

See [Appendix I on page 431](#) for examples of services. The following table describes the labels in this screen.

Table 90 Management > Bandwidth MGMT > Configuration

LABEL	DESCRIPTION
Active	Select this to enable bandwidth management.
LAN BW Budget(kbps)	<p>Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.</p> <p>It is recommended to set this speed to match what the LAN port's connection can handle. For example, set it to 100000 kbps if your Ethernet network has a maximum speed of 100000 kbps.</p> <p>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.</p> <p>You can also set this number lower than the interface's actual transmission speed. However, this will cause the ZyXEL Device to not use some of the interface's available bandwidth.</p>
WLAN BW Budget(kbps)	<p>Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.</p> <p>It is recommended to set this speed to match the maximum speed of the wireless network. In most cases, set it to 54000 kbps, unless your wireless network cannot handle this speed.</p> <p>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.</p> <p>You can also set this number lower than the interface's actual transmission speed. However, this will cause the ZyXEL Device to not use some of the interface's available bandwidth.</p>
WAN BW Budget(kbps)	<p>Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.</p> <p>It is recommended to set this speed to match what the WAN port's connection can handle. For example, set it to 40000 kbps if your broadband modem or router has a maximum speed of 40000 kbps.</p> <p>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.</p> <p>You can also set this number lower than the interface's actual transmission speed. However, this will cause the ZyXEL Device to not use some of the interface's available bandwidth.</p>
#	This field is a sequential value.
Direction	<p>Select LAN to apply bandwidth management to traffic that the ZyXEL Device forwards to the LAN.</p> <p>Select WAN to apply bandwidth management to traffic that the ZyXEL Device forwards to the WAN.</p> <p>Select WLAN to apply bandwidth management to traffic that the ZyXEL Device forwards to the WLAN.</p>
Name	This field displays the name of the rule. You can change it. Enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Service	This field displays one of the ZyXEL Device's predefined applications, or it displays User defined . If you want to change it to User defined , you may need to use the Edit Bandwidth Management Rule screen to set up detailed settings.
Dest Port	Enter the port number of the destination. A blank destination IP address means any destination IP address.

Table 90 Management > Bandwidth MGMT > Configuration (continued)

LABEL	DESCRIPTION
Priority	Select a priority from the drop down list box. Choose High , Mid or Low .
Modify	Use this field to edit or erase the rule. Click the Edit icon to open the Edit Bandwidth Management Rule screen. Click the Remove icon to erase this rule.
Apply	Click this to save the changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

15.3 Edit Bandwidth Management Rule Screen

Use this screen to create or edit bandwidth management rules. To open this screen, click an **Edit** icon in **Management > Bandwidth MGMT > Configuration**.

Figure 113 Management > Bandwidth MGMT > Configuration > Edit

Rule Configuration

Active

Rule Name

BW Budget (Kbps)

Priority

Use All Managed Bandwidth

Filter Configuration

Service

Destination Address

Destination Subnet Netmask

Destination Port

Source Address

Source Subnet Netmask

Source Port

Protocol

See [Appendix I on page 431](#) for examples of services. The following table describes the labels in this screen.

Table 91 Management > Bandwidth MGMT > Configuration > Edit

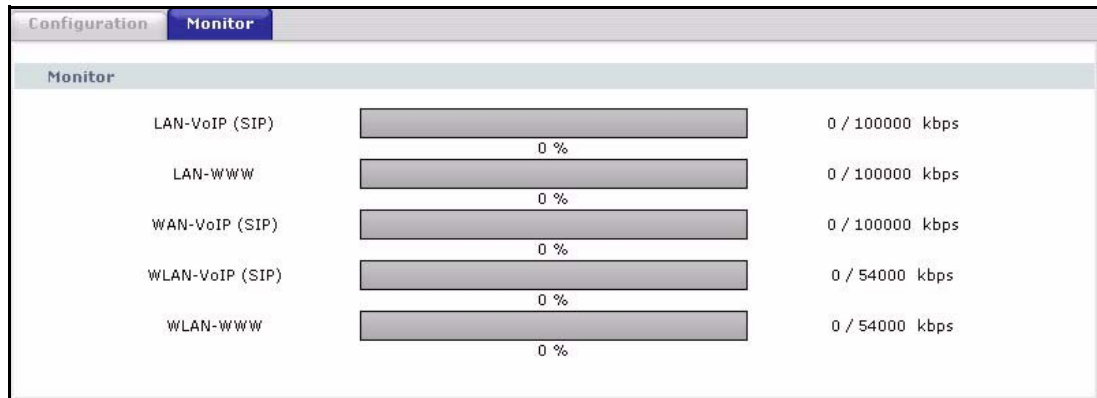
LABEL	DESCRIPTION
Rule Configuration	
Active	Select this to have the ZyXEL Device apply this bandwidth management rule. Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule. Enabling a bandwidth management rule also allows you to 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	
Service	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). SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select VoIP(SIP) from the drop-down list box to configure this bandwidth filter for traffic that uses SIP. 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. 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).
Destination Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Netmask	Enter the destination subnet mask. This field has no effect 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 has no effect 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.

Table 91 Management > Bandwidth MGMT > Configuration > Edit (continued)

LABEL	DESCRIPTION
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. A blank protocol ID means any protocol number.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

15.4 Bandwidth Monitor

Use this screen to view the ZyXEL Device's bandwidth usage and allotments. To open this screen, click **Management > Bandwidth MGMT > Monitor**.

Figure 114 Management > Bandwidth MGMT > Monitor

CHAPTER 16

Remote MGMT

Use these screens to control which computers can use which services to access the ZyXEL Device on each interface.

16.1 Remote Management Overview

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

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

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

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

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

- 1 Telnet
- 2 HTTP

16.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 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.
- 4 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.

16.1.2 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.

16.1.3 System Timeout

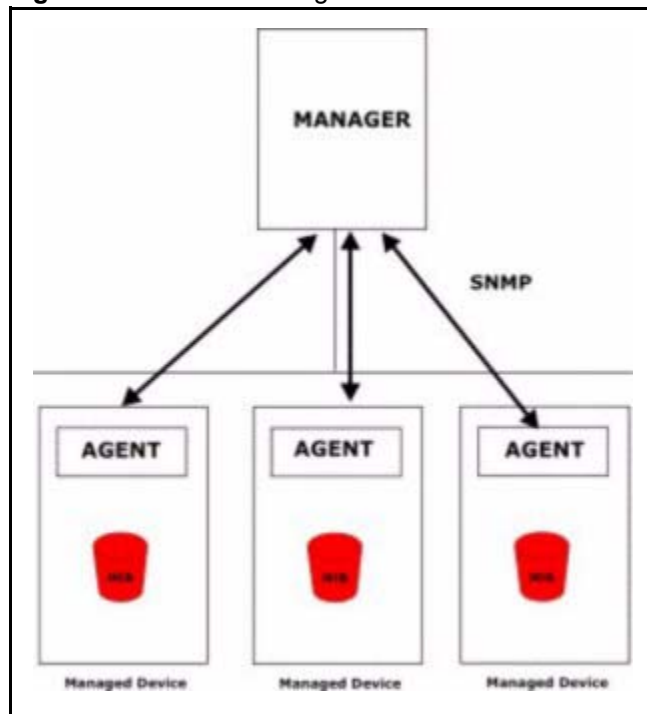
There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change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

16.1.4 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. SNMP is only available if TCP/IP is configured.

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

Figure 115 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.

16.1.4.1 Supported MIBs

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

16.1.4.2 SNMP Traps

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

Table 92 SNMPv1 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).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, 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.

Table 93 SNMPv2 Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Generic Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent after booting (power on). This trap is defined in RFC-1215.
warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent after booting (software reboot). This trap is defined in RFC-1215.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.13.0.1	This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CLI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the ZyXEL Device's physical ports.

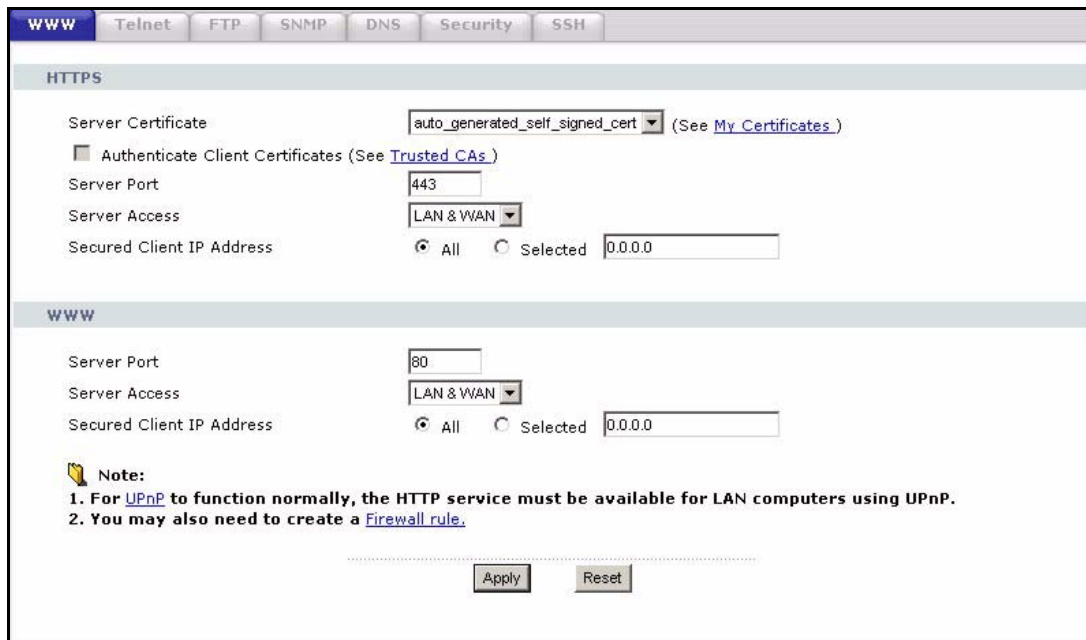
Table 94 SNMP Interface Index to Physical Port Mapping

INTERFACE TYPE	PHYSICAL PORT
enet0	WLAN
enet1	Ethernet port

16.2 WWW Screen

Use this screen to control HTTP access to your ZyXEL Device. To open this screen, click **Management > Remote MGMT > WWW**.

Figure 116 Management > Remote MGMT > WWW



Each field is described in the following table.

Table 95 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the certificate the ZyXEL Device provides to clients using this service.
Authenticate Client Certificates	This field is disabled if you have not set up any trusted certification authorities. Select this if you want the trusted certification authorities to check the clients' certificates before the ZyXEL Device allows access using this service.
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select All to allow any computer to access the ZyXEL Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
WWW	
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select All to allow any computer to access the ZyXEL Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

16.3 Telnet Screen

Use this screen to control Telnet access to your ZyXEL Device. To open this screen, click **Management > Remote MGMT > Telnet**.

Figure 117 Management > Remote MGMT > Telnet

Each field is described in the following table.

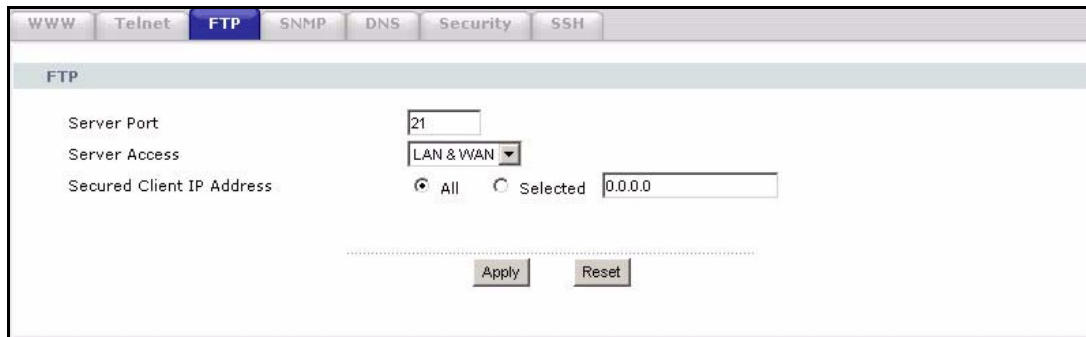
Table 96 Management > Remote MGMT > Telnet

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select All to allow any computer to access the ZyXEL Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

16.4 FTP Screen

Use this screen to control FTP access to your ZyXEL Device. To open this screen, click **Management > Remote MGMT > FTP**.

Figure 118 Management > Remote MGMT > FTP



Each field is described in the following table.

Table 97 Management > Remote MGMT > FTP

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select All to allow any computer to access the ZyXEL Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

16.5 SNMP Screen

Use this screen to control SNMP with your ZyXEL Device. To open this screen, click **Management > Remote MGMT > SNMP**.

Figure 119 Management > Remote MGMT > SNMP

Each field is described in the following table.

Table 98 Management > Remote MGMT > SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the password for incoming Get requests and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Type the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Type the IP address of the station to which send SNMP traps.
SNMP	
Service Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Service Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select All to allow any computer to access the ZyXEL Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

16.6 DNS Screen

Use this screen to control DNS access to your ZyXEL Device. To open this screen, click **Management > Remote MGMT > DNS**.

Figure 120 Management > Remote MGMT > DNS

The screenshot shows the DNS configuration page. At the top, there are navigation tabs: WWW, Telnet, FTP, SNMP, DNS (selected), Security, and SSH. Below the tabs, the page title is 'DNS'. The configuration area includes:

- Service Port:** A text input field containing the value '53'.
- Service Access:** A dropdown menu currently set to 'LAN & WAN'.
- Secured Client IP Address:** Radio buttons for 'All' (selected) and 'Selected', followed by a text input field containing '0.0.0.0'.

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

Each field is described in the following table.

Table 99 Management > Remote MGMT > DNS

LABEL	DESCRIPTION
Server Port	This field is read-only. It displays the port number this service uses to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select All to allow any computer to access the ZyXEL Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

16.7 Security Screen

Use this screen to control how your ZyXEL Device responds to other types of requests. To access this screen, click **Management > Remote MGMT > Security**.

Figure 121 Management > Remote MGMT > Security

The screenshot shows the Security configuration page. At the top, there are navigation tabs: WWW, Telnet, FTP, SNMP, DNS, Security (selected), and SSH. Below the tabs, the page title is 'ICMP'. The configuration area includes:

- Respond to Ping on:** A dropdown menu currently set to 'LAN & WAN'.
- Do not respond to requests for unauthorized services:** An unchecked checkbox.

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

Each field is described in the following table.

Table 100 Management > Remote MGMT > Security

LABEL	DESCRIPTION
Respond to Ping on	Select the interface(s) on which the ZyXEL Device should respond to incoming ping requests. Disable - the ZyXEL Device does not respond to any ping requests. LAN - the ZyXEL Device only responds to ping requests received from the LAN. WAN - the ZyXEL Device only responds to ping requests received from the WAN. LAN & WAN - the ZyXEL Device responds to ping requests received from the LAN or the WAN.
Do not respond to requests for unauthorized services	Select this to prevent outsiders from discovering your ZyXEL Device by sending requests to unsupported port numbers. 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. If you clear this, your ZyXEL Device replies with an ICMP Port Unreachable packet for a port probe on unused UDP ports and with a TCP Reset packet for a port probe on unused TCP ports.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

16.8 SSH Screen

Use this screen to control SSH access to your ZyXEL Device. To open this screen, click **Management > Remote MGMT > SSH**.

Figure 122 Management > Remote MGMT > SSH

The screenshot shows the SSH configuration page with the following fields and values:

- Server Host Key: auto_generated_self_signed_cert (See My Certificates)
- Server Port: 22
- Server Access: LAN & WAN
- Secured Client IP Address: All Selected 0.0.0.0

Note: You may also need to create a [Firewall rule](#).

Buttons: Apply, Reset

Each field is described in the following table.

Table 101 Management > Remote MGMT > SSH

LABEL	DESCRIPTION
Server Host Key	Select the certificate the ZyXEL Device provides to clients using this service.
Server Port	This field is read-only. It displays the port number this service uses to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select All to allow any computer to access the ZyXEL Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

16.9 TR-069

TR-069 is a protocol that defines how your ZyXEL Device can be managed via a management server such as ZyXEL's Vantage CNM Access.

An administrator can use CNM Access to remotely set up the ZyXEL device, modify settings, perform firmware upgrades as well as monitor and diagnose the ZyXEL device. All you have to do is enable the device to be managed by CNM Access and specify the CNM Access IP address or domain name and username and password.

Follow the procedure below to configure your ZyXEL Device to be managed by CNM Access. See the Command Interpreter appendix for information on the command structure and how to access the CLI (Command Line Interface) on the ZyXEL Device.

Note: In this example **a.b.c.d** is the IP address of CNM Access. You must change this value to reflect your actual management server IP address or domain name. See [Table 102 on page 216](#) for detailed descriptions of the commands.

Figure 123 Enabling TR-069

```

ras> wan tr069 load
ras> wan tr069 acsUrl a.b.c.d
Auto-Configuration Server URL: http://a.b.c.d
ras> wan tr069 periodicEnable 1
ras> wan tr069 informInterval 2400
TR069 Informinterval 2400
ras> wan tr069 active 1
ras> wan tr069 save

```

The following table gives a description of TR-069 commands.

Table 102 TR-069 Commands

Root	Command or Subdirectory	Command	Description
wan	tr069		All TR-069 related commands must be preceded by <code>wan tr069</code> .
		<code>load</code>	Start configuring TR-069 on your ZyXEL Device.
		<code>active [0:no/ 1:yes]</code>	Enable/disable TR-069 operation.
		<code>acsUrl <URL></code>	Set the IP address or domain name of CNM Access.
		<code>username [maxlength:15]</code>	Username used to authenticate the device when making a connection to CNM Access. This username is set up on the server and must be provided by the CNM Access administrator.
		<code>password [maxlength:15]</code>	Password used to authenticate the device when making a connection to CNM Access. This password is set up on the server and must be provided by the CNM Access administrator.
		<code>periodicEnable [0:Disable/ 1:Enable]</code>	Whether or not the device must periodically send information to CNM Access. It is recommended to set this value to <code>1</code> in order for the ZyXEL Device to send information to CNM Access.
		<code>informInterval [sec]</code>	The duration in seconds of the interval for which the device MUST attempt to connect with CNM Access to send information and check for configuration updates. Enter a value between 30 and 2147483647 seconds.
		<code>save</code>	Save the TR-069 settings to your ZyXEL Device.

CHAPTER 17

UPnP

This chapter introduces the Universal Plug-and-Play (UPnP) feature.

17.1 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.

17.1.1 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.

17.1.2 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.

17.1.3 Cautions with UPnP

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

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

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

17.2 UPnP and ZyXEL

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

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

17.3 UPnP Screen

Use this screen to set up UPnP on your ZyXEL Device. To open this screen, click **Management > UPnP > General**.

Figure 124 Management > UPnP

The following table describes the fields in this screen.

Table 103 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this 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 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.

Table 103 Configuring UPnP

LABEL	DESCRIPTION
Allow UPnP to pass through Firewall	Select this to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click this to save the setting to the ZyXEL Device.
Reset	Click this to return to the previously saved settings.

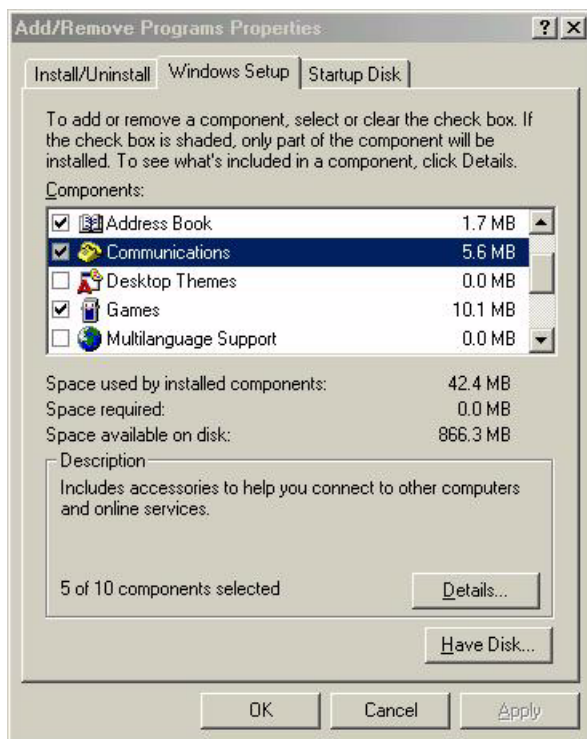
17.4 Installing UPnP in Windows Example

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

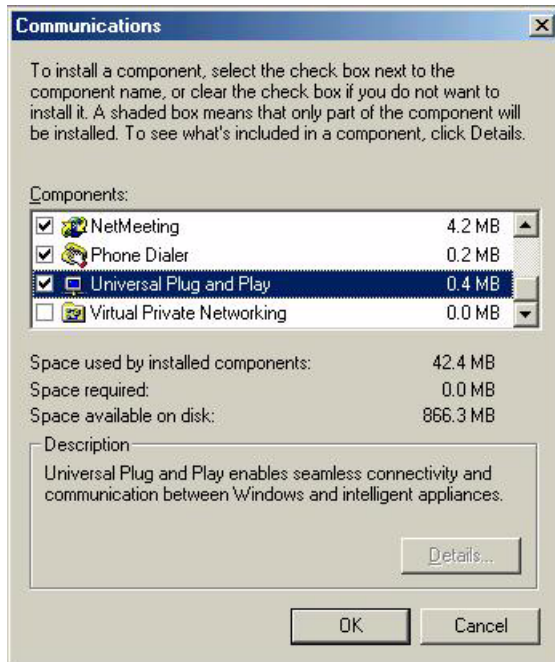
Installing UPnP in Windows Me

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 125 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 126 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

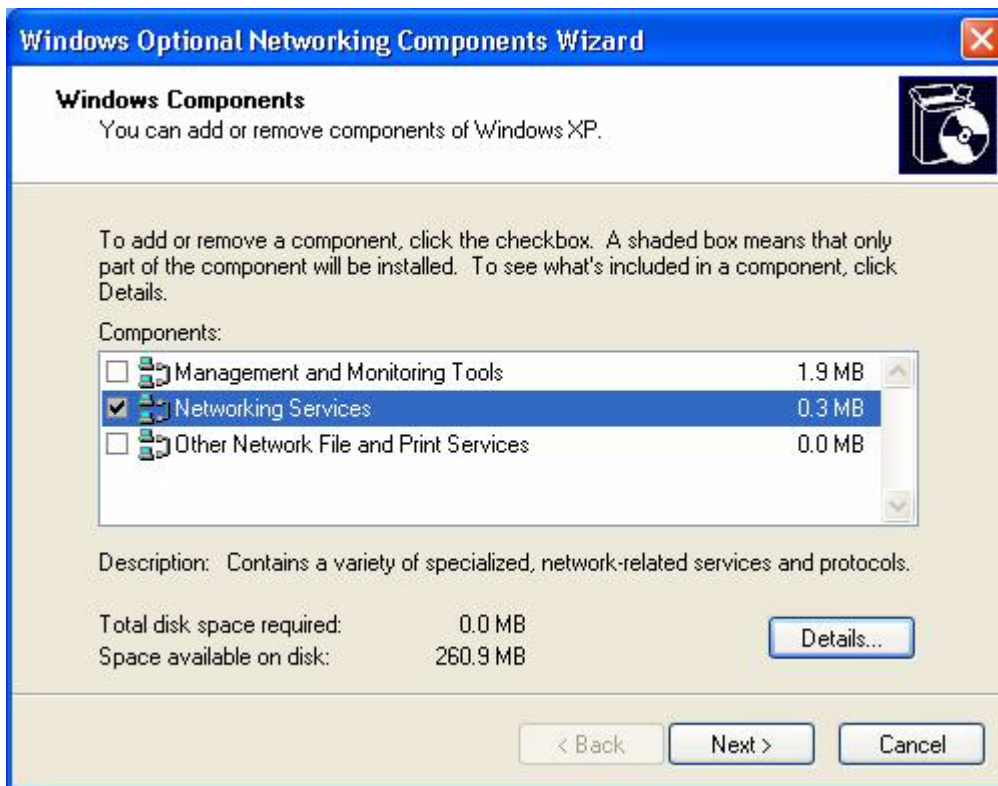
Follow the steps below to install the UPnP in Windows XP.

- 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 127 Network Connections

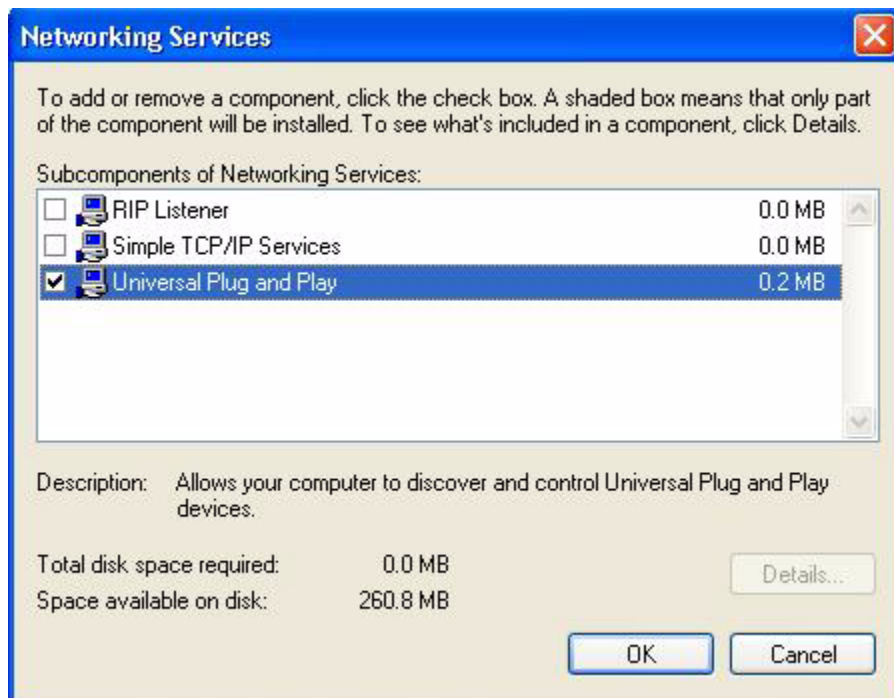
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 128 Windows Optional Networking Components Wizard



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

Figure 129 Networking Services



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

17.5 Using UPnP in Windows XP Example

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

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

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**.

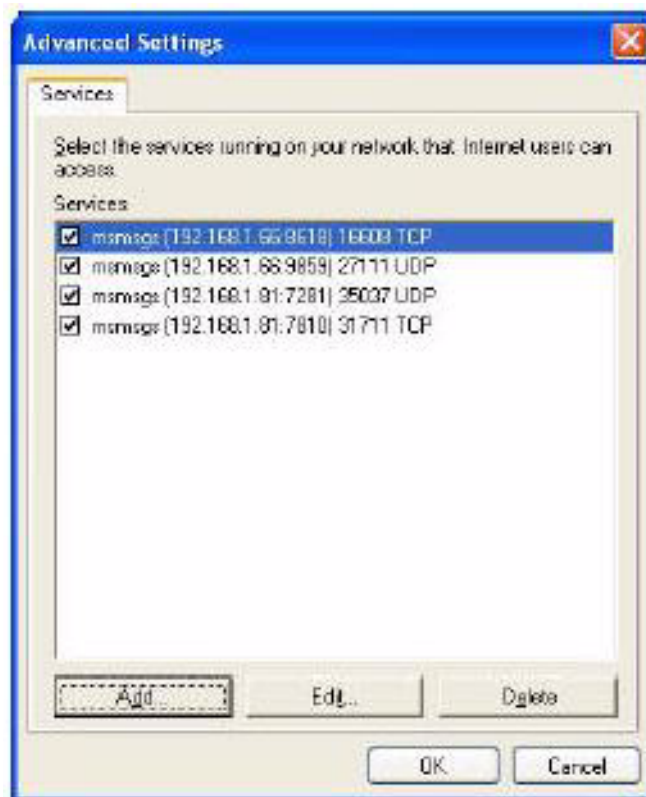
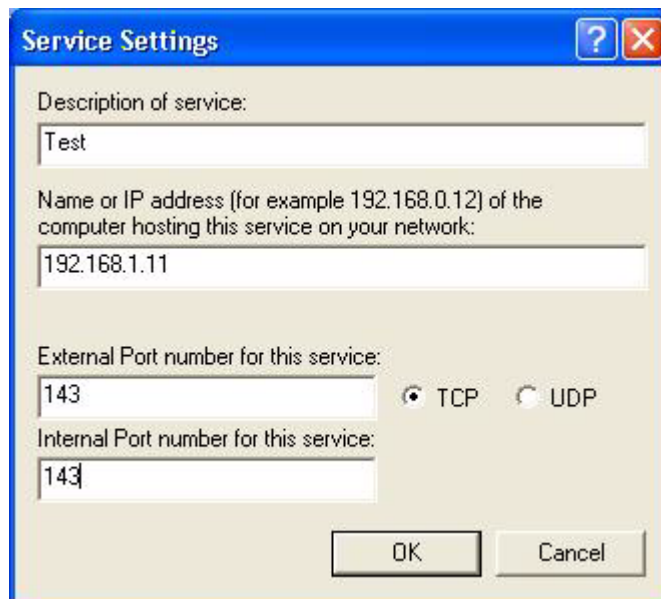
Figure 130 Network Connections



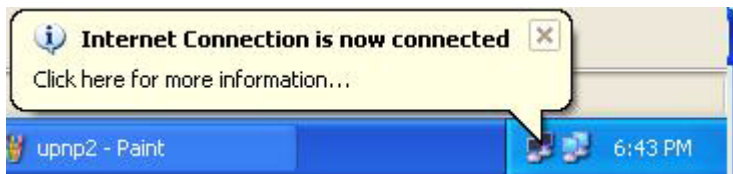
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 131 Internet Connection Properties

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

Figure 132 Internet Connection Properties: Advanced Settings**Figure 133** 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 134 System Tray Icon

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

Figure 135 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.

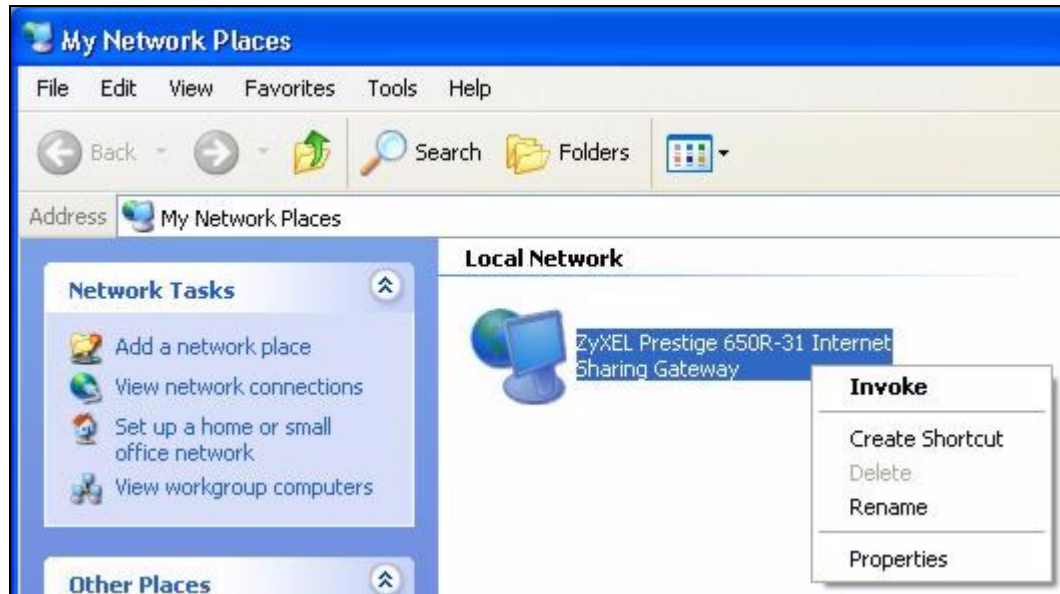
Follow the steps below to access the web configurator.

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

Figure 136 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 137 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 138 Network Connections: My Network Places: Properties: Example

CHAPTER 18

System

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

18.1 General Setup

18.1.1 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**.

18.1.2 Dynamic DNS Overview

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

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

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.

18.1.2.1 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.

18.1.3 Resetting the Time

If you use a time server, the ZyXEL Device updates the current date and time when the ZyXEL Device starts up and in 24-hour intervals after that (until you turn off the ZyXEL Device).

If you update the current date and time manually, the ZyXEL Device updates the current date and time when you save changes in **Maintenance > System > Time Setting** or SMT menu 24.10 (see [Section 36.4 on page 335](#)).

18.2 General System Screen

Use this screen to set up basic system parameters and to change the password. To open this screen, click **Maintenance > System > General**.

Figure 139 Maintenance > System > General

The following table describes the labels in this screen.

Table 104 Maintenance > System > General

LABEL	DESCRIPTION
System 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.

Table 104 Maintenance > System > General (continued)

LABEL	DESCRIPTION
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 CLI (Command Line Interpreter)) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	
Old Password	Type the current password you use to access the system.
New Password	Type the new system password (up to 30 characters). As you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

18.3 Dynamic DNS Screen

Use this screen to set up and maintain dynamic DNS on your ZyXEL Device. To open this screen, click **Maintenance > System > Dynamic DNS**.

Figure 140 Maintenance > System > Dynamic DNS

The following table describes the fields in this screen.

Table 105 Maintenance > System > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Enable Dynamic DNS	Select this to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service for which you are registered 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; separate them with a comma (,).
User Name	Type the user name for your Dynamic DNS account.
Password	Type the password for your Dynamic DNS account.
Enable Wildcard Option	Select this to enable DynDNS Wildcard.
Enable off line option	This option is available when Custom DNS 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 to assign the WAN IP address for the host name(s).

Table 105 Maintenance > System > Dynamic DNS (continued)

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP Address	Select this only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. With this feature, the DDNS server automatically detects and uses the IP address of the appropriate 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	Select this if you have a static IP address, and type the IP address for the host name(s).
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

18.4 Time Setting Screen

Use this screen to change the current time and time settings on your ZyXEL Device. To open this screen, click **Maintenance > System > Time Setting**.

Figure 141 Maintenance > System > Time Setting

The following table describes the fields in this screen.

Table 106 Maintenance > 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.
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 uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, NTP (RFC 1305) , is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.

Table 106 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Start Date	<p>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:</p> <p>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.</p> <p>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).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Enable Daylight Saving. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Last, Sunday, October and type 2 in the o'clock field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October. The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

CHAPTER 19

Logs

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

19.1 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.

19.1.1 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.

19.2 View Log Screen

Use this screen to look at log messages recorded by your ZyXEL Device. To open this screen, click **Maintenance > Logs > View Log**.

Figure 142 Maintenance > Logs > View Log

#	Time	Message	Source	Destination	Note
1	2000-01-01 03:46:50	WLAN STA Association			MACAddr:00:12:0e:2c:49:3d
2	2000-01-01 03:19:39	WLAN STA Association Again			MACAddr:00:11:e0:ff:80:07
3	2000-01-01 03:19:38	WLAN STA Association			MACAddr:00:11:e0:ff:80:07
4	2000-01-01 03:18:36	WLAN STA Association Again			MACAddr:00:a0:c5:40:c2:a1
5	2000-01-01 03:15:42	WLAN STA Association Again			MACAddr:00:a0:c5:40:c2:a1

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills up. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order. The following table describes the fields in this screen.

Table 107 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	Select a category of logs to view; select All Logs to look at logs. The drop-down list box only lists categories that you select in the Log Settings screen.
Email Log Now	Click this 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 this to update the screen.
Clear Log	Click this to delete all the logs, regardless of which ones are shown.
#	This field is a sequential value, and it is not associated with any log.
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.
Note	This field displays additional information about the log entry.

19.3 Log Settings Screen

Use this 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. To open this screen, click **Maintenance > Logs > Log Settings**.

Figure 143 Maintenance > Logs > Log Settings

The following table describes the fields in this screen.

Table 108 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 108 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. 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 p.m.) 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 can send logs 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 the file the syslog server uses for the ZyXEL Device. 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	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.
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 this to save your customized settings and exit this screen.
Reset	Click this to return to the previously saved settings.

CHAPTER 20

Tools

This chapter upload new firmware, manage configuration and restart your ZyXEL Device.

20.1 Firmware Upgrade

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "Prestige.bin". Only use firmware for your device's specific model. Refer to the label on the bottom of your device.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

To open this screen, click **Maintenance > Tools > Firmware**.

Figure 144 Maintenance > Tools > Firmware

The following table describes the labels in this screen.

Table 109 Maintenance > Tools > Firmware

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 this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this 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 click **Upload**, the following screen appears.

Figure 145 Upload Firmware: In Progress

Wait two minutes before logging into the ZyXEL Device again. The ZyXEL Device automatically restarts in this time, which causes a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 146 Upload Firmware: Network Temporarily Disconnected

Log in again, and check your new firmware version in the **Status** screen.

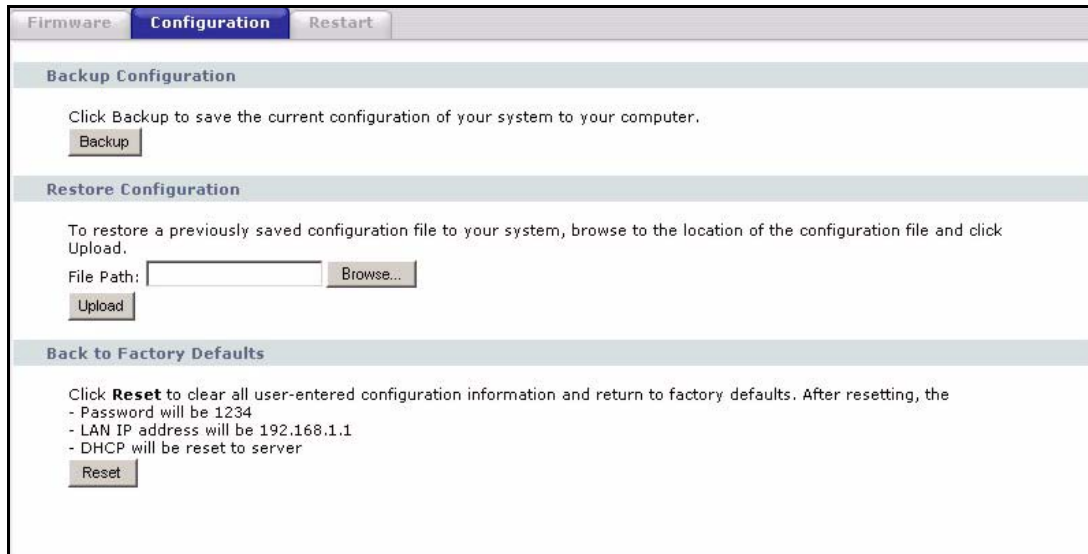
If the upload was not successful, the following screen appears. Click **Return** to go back to the **Maintenance > Tools > Firmware** screen.

Figure 147 Upload Firmware: Error

20.2 Configuration Screen

Use this screen to back up and restore the configuration of the ZyXEL Device and to reset the configuration to the factory-default settings. To open this screen, click **Maintenance > Tools > Configuration**.

Figure 148 Maintenance > Tools > Configuration



The following table describes each field in the screen.

Table 110 Maintenance > Tools > Configuration

LABEL	DESCRIPTION
Backup Configuration	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.
Backup	Click this to save the ZyXEL Device's current configuration to your computer.
Restore Configuration	
File Path	Type in the location of the file you want to upload in this field or click Browse... to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process. See below for more information about this process.
Back to Factory Defaults	
Reset	Click this to clear all user-entered configuration information and returns the ZyXEL Device to its factory defaults. This is the same as pressing the RESET button on the back of your ZyXEL Device.

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

After you click **Upload**, the following screen appears.

Figure 149 Restore Configuration: Successful

Wait one minute before logging into the ZyXEL Device again. The ZyXEL Device automatically restarts in this time, which causes a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 150 Restore Configuration: Network Temporarily Disconnected

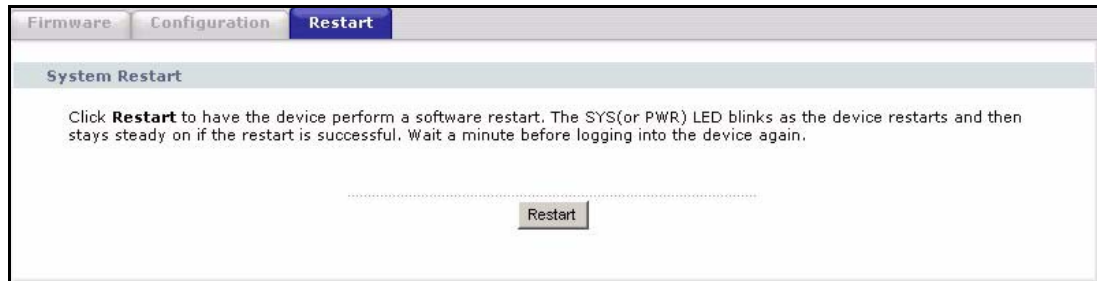
If the IP address of the ZyXEL Device is different in the new configuration, you may need to change the IP address in your browser and maybe put your computer in the same subnet as the ZyXEL Device. See the appendix for details on how to set up your computer's IP address.

If the upload was not successful, the following screen appears. Click **Return** to go back to the **Maintenance > Tools > Configuration** screen.

Figure 151 Restore Configuration: Error

20.3 Restart Screen

Use this screen to reboot the ZyXEL Device without turning the power off. This does not affect the ZyXEL Device's configuration. To open this screen, click **Maintenance > Tools > Restart**.

Figure 152 Restart Screen

Click **Restart** to have the ZyXEL Device reboot.

CHAPTER 21

Introducing the SMT

The System Management Terminal (SMT) provides a text-based, menu-driven console to manage the ZyXEL Device. This chapter describes how to access the SMT and then provides an overview of its menus.

21.1 Accessing the SMT

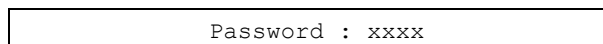
Use Telnet to access the SMT. Follow these steps.

- 1 In Windows, click **Start > Run**.
- 2 Type “telnet [w.x.y.z](#)”, and click **OK**.

[w.x.y.z](#) is the IP address of the ZyXEL Device; the default address is 192.168.1.1.

The ZyXEL Device prompts you for the password.

Figure 153 Login Screen



```
Password : xxxx
```

- 3 Enter the password. The default password is 1234. As you type the password, the screen displays an asterisk “*” for each character you type.
- 4 After you enter the password, the SMT main menu appears, as shown next.

Note: Use menu 23.1 to change the password.

Figure 154 SMT Main Menu

```

Copyright (c) 1994 - 2003 ZyXEL Communications Corp.

P-870HW-I1 Main Menu

Getting Started
  1. General Setup
  2. WAN Setup
  3. LAN Setup
  4. Internet Access Setup

Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup
  14. Dial-in User Setup
  15. NAT Setup

Advanced Management
  21. Filter and Firewall Setup
  22. SNMP Configuration
  23. System Security
  24. System Maintenance
  25. IP Routing Policy Setup
  26. Schedule Setup

99. Exit

Enter Menu Selection Number:

```

Note: There is an inactivity timeout, and the default value is five minutes. If there is no activity for longer than five minutes, your ZyXEL Device will automatically log you out. You will then have to telnet into the ZyXEL Device again. You can use the web configurator or the CLI commands (menu 24.8) to change the inactivity timeout period.

21.2 SMT Menu Items

The following table provides an overview of each menu item.

Table 111 SMT Menus Overview

MENUS	SUB MENU	DESCRIPTION
1 General Setup		Use this menu to set up the system name, domain name, and DNS servers.
1.1 Configure Dynamic DNS		Use this menu to configure your dynamic DNS account settings.
	1.1.1 DDNS Edit Host	Use this menu to configure your dynamic DNS domain name settings.
2 WAN Setup		Use this menu to configure the WAN MAC address.
3 LAN Setup		
3.1 LAN Port Filter Setup		Use this menu to specify input and output filter sets for the LAN port.

Table 111 SMT Menus Overview (continued)

MENUS	SUB MENUS	DESCRIPTION
3.2 TCP/IP and DHCP Ethernet Setup		Use this menu to set up the LAN IP address and to configure the ZyXEL Device's DHCP server. The DHCP server assigns IP addresses and provides DNS server information to other computers on the LAN or WLAN.
	3.2.1 IP Alias Setup	Use this menu to partition your LAN interface into subnets.
3.5 Wireless LAN Setup		Use this menu to configure basic wireless settings and wireless security.
	3.5.1 WLAN MAC Address Filter	Use this menu to block or allow other devices to access the ZyXEL Device.
4 Internet Access Setup		Use this menu to set up your Internet connection. Use Menu 11 instead if you want to set up advanced features too.
11 Remote Node Setup		
11.1 Remote Node Profile		Use this menu to set up your Internet connection.
	11.1.2 Remote Node Network Layer Options	Use this menu to set up the WAN IP address and advanced features for the WAN port.
	11.1.4 Remote Node Filter	Use this menu to specify input and output filter sets for the WAN port.
	11.1.5 Traffic Redirect Setup	Use this menu to set up a backup router, if you have one, in case the ZyXEL Device cannot access the Internet.
12 Static Routing Setup		Use this menu to look at IP static routes.
12.1 Edit IP Static Route		Use this menu to configure IP static routes.
14 Dial-in User Setup		Use this menu to look at local user profiles on the ZyXEL Device.
14.1 Edit Dial-in User		Use this menu to configure local user profiles on the ZyXEL Device.
15 NAT Setup		
15.1 Address Mapping Sets		Use this menu to select which address mapping set you want to configure.
	15.1.1 Address Mapping Rules	Use this menu to look at network address translation mapping rules.
	15.1.1.1 Address Mapping Rule	Use this menu to configure network address translation mapping rules.
15.2 NAT Server Setup		Use this menu to look at servers for which you have configured port forwarding rules.
	15.2.1 NAT Server Configuration	Use this menu to configure port forwarding rules for servers behind the ZyXEL Device.
15.3 Trigger Port Setup	s	Use this menu to change your ZyXEL Device's port triggering settings.
21 Filter and Firewall Setup		

Table 111 SMT Menus Overview (continued)

MENUS	SUB MENUS	DESCRIPTION
21.1 Filter Set Configuration		Use this menu to look at the filter sets in the ZyXEL Device.
	21.1.x Filter Rules Summary	Use this menu to look at the rules for each filter set.
	21.1.x.y TCP/IP Filter Rule	Use this menu to configure the rules for each filter set.
21.2 Firewall Setup		Use this menu to activate or deactivate the firewall.
22 SNMP Configuration		Use this menu to configure your ZyXEL Device's settings for Simple Network Management Protocol (SNMP) management.
23 System Security		
23.1 Change Password		Use this menu to change the administrator password for the ZyXEL Device.
23.2 RADIUS Server		Use this menu to configure a RADIUS server to use for wireless user authentication.
23.4 IEEE802.1X		Use this menu to configure IEEE 802.1x wireless authentication for the ZyXEL Device.
24 System Maintenance		
24.1 System Status		Use this menu to look at packet statistics, interface status, and basic device information.
24.2 System Information and Console Port Speed		
	24.2.1 Information	Use this menu to look at basic device information and LAN interface settings.
	24.2.2 Change Console Port Speed	Use this menu to change the console port speed.
24.3 Log and Trace		
	24.3.2 Syslog Logging	Use this menu to configure the ZyXEL Device to send log messages to a syslog server.
	24.3.4 Call-Triggering Packet	Use this menu to look at information about the packet that triggered a dial-out call.
24.4 Diagnostic		Use this menu to check the ZyXEL Device's connections to other devices.
24.5 Backup Configuration		Use this menu to get instructions for backing up the current configuration of the ZyXEL Device.
24.6 Restore Configuration		Use this menu to get instructions for restoring a previously-saved configuration of the ZyXEL Device.
24.7 Upload Firmware		
	24.7.1 Upload System Firmware	Use this menu to get instructions for loading new firmware.
	24.7.2 Upload System Configuration File	Use this menu to get instructions for restoring the system configuration of the ZyXEL Device. This sets the configuration to its default values.

Table 111 SMT Menus Overview (continued)

MENUS	SUB MENUS	DESCRIPTION
24.8 Command Interpreter Mode		Use this menu to use CI commands.
24.9 Call Control		
	24.9.1 Budget Management	Use this menu to look at how long you have accessed the Internet and how much budgeted time remains.
	24.9.2 Call History	Use this menu to look at previous calls made to establish the Internet connection.
24.10 Time and Date Setting		Use this menu to change your ZyXEL Device's time and date.
24.11 Remote Management Control		Use this screen to configure through which interface(s) and from which IP address(es) users can use various protocols to manage the ZyXEL Device.
25 IP Routing Policy Summary		Use this menu to look at policy routes.
25.1 IP Routing Policy Setup		Use this menu to configure policy routes.
	25.1.1 IP Routing Policy Setup	Use this menu to specify the ports from which traffic comes to which the policy routes apply.
26 Schedule Setup		Use this menu to look at the schedule sets in the ZyXEL Device.
26.1 Schedule Set Setup		Use this menu to configure the schedule sets in the ZyXEL Device.
99 Exit		Use this menu to close the SMT.

21.3 Navigating the SMT Interface

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 112 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change No to Yes then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of No . Press [SPACE BAR] once to change No to Yes , then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.

Table 112 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?> or ChangeMe	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with ChangeMe must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

CHAPTER 22

General Setup

Use this menu to set up the system name, domain name, DNS servers, and dynamic DNS.

22.1 General Setup

Use this menu to set up the system name, domain name, and DNS servers. See [Chapter 18 on page 229](#) and [Chapter 7 on page 119](#) for background information. To open this menu, enter 1 in the main menu.

Figure 155 Menu 1: General Setup

```

Menu 1 - General Setup

System Name= P870HW-I1
Domain Name=

First System DNS Server= From ISP
IP Address= N/A
Second System DNS Server= From ISP
IP Address= N/A
Third System DNS Server= From ISP
IP Address= N/A
Edit Dynamic DNS= No

```

The following table describes the labels in this menu.

Table 113 Menu 1: General Setup

FIELD	DESCRIPTION
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.
	DNS (Domain Name System) manages the relationships between domain names and IP addresses. For example, the IP address of www.zyxel.com is 204.217.0.2. Without a DNS server, you must know the IP address of the computer you want to access before you access it. The ZyXEL Device uses a system DNS server to resolve domain names for DDNS and the time server.

Table 113 Menu 1: General Setup (continued)

FIELD	DESCRIPTION
First System DNS Server	Press [SPACE BAR] to select From ISP , User Defined or None and press [ENTER]. These fields are not available on all models.
Second System DNS Server	Select From ISP if your ISP dynamically assigns DNS server information. (In this case, the ISP assigns the WAN IP address too. See Menu 4 .) The field to the right is read-only, and it displays the IP address provided by your ISP.
Third System DNS Server	Select User-Defined if you have the IP address of a DNS server. You might get it from your ISP or from your network. Enter the IP address in the field below. Select None if you do not want to use this DNS server. If you select None for all of the DNS servers, you must use IP addresses to configure the ZyXEL Device and to access the Internet.
IP Address	Enter the IP addresses of the DNS servers. This field is available when you select User-Defined in the field above.
Edit Dynamic DNS	If you want to set up dynamic DNS, press [SPACE BAR] to select Yes and press [ENTER]. Menu 1.1 appears.

22.2 Configure Dynamic DNS

Use this menu to configure your dynamic DNS account settings. See [Chapter 18 on page 229](#) for background information. To open this menu, select **Yes** in **Edit Dynamic DNS** in menu 1.

Figure 156 Menu 1.1: Configure Dynamic DNS

Menu 1.1 - Configure Dynamic DNS	
Service Provider=	WWW.DynDNS.ORG
Active=	No
Username=	
Password=	*****
Edit Host=	No

The following table describes the labels in this menu.

Table 114 Menu 1.1: Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	Select the name of your Dynamic DNS service provider.
Active	Select Yes to use dynamic DNS.
Username	Type the user name for your Dynamic DNS account.
Password	Type the password for your Dynamic DNS account.
Edit Host	If you want to set up a domain name to use with your dynamic DNS account, press [SPACE BAR] to select Yes and press [ENTER]. Menu 1.1.1 appears.

22.3 Configure Dynamic DNS

Use this menu to configure your dynamic DNS domain name settings. See [Chapter 18 on page 229](#) for background information. To open this menu, select **Yes** in **Edit Host** in menu 1.1.

Figure 157 Menu 1.1.1: DDNS Edit Host

```

Menu 1.1.1 - DDNS Edit Host

Hostname=
DDNS Type= DynamicDNS
Enable Wildcard Option= No
Enable Off Line Option= N/A
IP Address Update Policy:
  Let DDNS Server Auto Detect= No
  Use User-Defined= No
  Use WAN IP Address= N/A

```

The following table describes the labels in this menu.

Table 115 Menu 1.1.1: DDNS Edit Host

FIELD	DESCRIPTION
Hostname	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.
DDNS Type	Select the type of service for which you are registered from your Dynamic DNS service provider.
Enable Wildcard Option	Select this 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	If you do not select either option below, the ZyXEL Device uses the WAN IP address for the domain name.
Let DDNS Server Auto Detect	Select this only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. With this feature, the DDNS server automatically detects and uses the IP address of the appropriate 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 User-Defined	Select this if you have a static IP address, and type the IP address for the host name(s) in the Use WAN IP Address field.
Use WAN IP Address	Select Use User-Defined if you have a static IP address, and type the IP address for the host name(s) in this field.

CHAPTER 23

WAN Setup

Use this menu to configure the WAN MAC address. See [Chapter 7 on page 119](#) for background information. To open this menu, enter 2 in the main menu.

Figure 158 Menu 2: WAN Setup

Menu 2 - WAN Setup MAC Address: Assigned By= Factory default IP Address= N/A

The following table describes the labels in this menu.

Table 116 Menu 2: WAN Setup

FIELD	DESCRIPTION
MAC Address	
Assigned By	Select IP address attached on LAN if you want the ZyXEL Device to use the MAC address of another computer, instead of its default MAC address. You might try this if you lose your Internet connection because some ISPs check the MAC address of the device connected to the Internet. Otherwise, select Factory default .
IP Address	If you select IP address attached on LAN in the Assigned By field, enter the IP address of the computer whose MAC address you want the ZyXEL Device to use.

CHAPTER 24

LAN Setup

Use this menu to set up the LAN IP address, DHCP server, additional subnets, and input and output filter sets for the LAN port. You can also use this menu to configure the wireless network.

24.1 LAN Port Filter Setup

Use this menu to specify input and output filter sets for the LAN port. See [Chapter 30 on page 287](#) for background information. To open this menu, enter 1 in menu 3.

Figure 159 Menu 3.1: LAN Port Filter Setup

```

Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

```

The following table describes the labels in this menu.

Table 117 Menu 3.1: LAN Port Filter Setup

FIELD	DESCRIPTION
Input Filter Sets	
protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
device filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
Output Filter Sets	
protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
device filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).

24.2 TCP/IP and DHCP Ethernet Setup

Use this menu to set up the LAN IP address and to configure the ZyXEL Device's DHCP server. The DHCP server assigns IP addresses and provides DNS server information to other computers on the LAN or WLAN. See [Chapter 8 on page 127](#) and [Chapter 9 on page 133](#) for background information. To open this menu, enter 2 in menu 3.

Figure 160 Menu 3.2: TCP/IP and DHCP Ethernet Setup

Menu 3.2 - TCP/IP and DHCP Ethernet Setup	
DHCP= Server	TCP/IP Setup:
Client IP Pool:	IP Address= 192.168.1.1
Starting Address= 192.168.1.33	IP Subnet Mask= 255.255.255.0
Size of Client IP Pool= 6	RIP Direction= Both
First DNS Server= From ISP	Version= RIP-1
IP Address= N/A	Multicast= None
Second DNS Server= From ISP	Edit IP Alias= No
IP Address= N/A	
Third DNS Server= From ISP	
IP Address= N/A	
DHCP Server Address= N/A	

The following table describes the labels in this menu.

Table 118 Menu 3.2: TCP/IP and DHCP Ethernet Setup

FIELD	DESCRIPTION
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.
Client IP Pool	These fields are available if you select Server in the DHCP field.
Starting Address	Enter the IP address from which the ZyXEL Device begins allocating IP addresses. You can assign a static IP address to a specific computer; see Network > DHCP Server > Static DHCP .
Size of Client IP Pool	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the subnet mask 255.255.255.0. For example, if the IP Pool Start Address is 10.10.10.10, the ZyXEL Device can allocate up to 10.10.10.254, or 245 IP addresses.
	These fields are available if you select Server in the DHCP field. The ZyXEL Device provides the following DNS servers to DHCP clients.

Table 118 Menu 3.2: TCP/IP and DHCP Ethernet Setup (continued)

FIELD	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	<p>Press [SPACE BAR] to select From ISP, User Defined or None and press [ENTER]. These fields are not available on all models.</p> <p>Select From ISP if your ISP dynamically assigns DNS server information. (In this case, the ISP assigns the WAN IP address too. See Menu 4.) The field to the right is read-only, and it displays the IP address provided by your ISP.</p> <p>Select User-Defined if you have the IP address of a DNS server. You might get it from your ISP or from your network. Enter the IP address in the field below.</p> <p>Select None if you do not want to use this DNS server. If you select None for all of the DNS servers, you must use IP addresses to configure the ZyXEL Device and to access the Internet.</p> <p>Select DNS Relay if you want to use the ZyXEL Device's IP address. In this case, the ZyXEL Device finds out the IP address of the DNS server (based on RFC 1877). Then, it forwards DNS queries from DHCP clients to this server and sends the response back to the DHCP clients.</p>
IP Address	If you select User-Defined in the field above, enter the IP address of the DNS server in this field.
DHCP Server Address	This field is available if you select Relay in the DHCP field. Enter the IP address of the DHCP server for the network.
TCP/IP Setup	
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 or network administrator. If they did not provide one, use the default value.
RIP Direction	<p>Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet.</p> <p>None - The ZyXEL Device does not send or receive routing information on the subnet.</p> <p>Both - The ZyXEL Device sends and receives routing information on the subnet.</p> <p>In Only - The ZyXEL Device only receives routing information on the subnet.</p> <p>Out Only - The ZyXEL Device only sends routing information on the subnet.</p>
Version	<p>Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet.</p> <p>RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information.</p> <p>RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information.</p> <p>RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.</p>
Multicast	<p>You do not have to enable multicasting to use RIP-2M. (See RIP Version.)</p> <p>Select which version of IGMP the ZyXEL Device uses to support multicasting on the LAN. Multicasting sends packets to some computers on the LAN and is an alternative to unicasting (sending packets to one computer) and broadcasting (sending packets to every computer).</p> <p>None - The ZyXEL Device does not support multicasting.</p> <p>IGMP-v1 - The ZyXEL Device supports IGMP version 1.</p> <p>IGMP-v2 - The ZyXEL Device supports IGMP version 2.</p> <p>Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers on the LAN have to support the same version of IGMP.</p>
Edit IP Alias	If you want to partition your LAN interface into subnets, press [SPACE BAR] to select Yes and press [ENTER]. Menu 3.2.1 appears.

24.3 IP Alias Setup

Use this menu to partition your LAN interface into subnets. See [Chapter 8 on page 127](#) and [Chapter 30 on page 287](#) for background information. To open this menu, select **Yes** in **Edit IP Alias** in menu 3.2.

Figure 161 Menu 3.2.1: IP Alias Setup

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
  Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A
IP Alias 2= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
  Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A

```

The following table describes the labels in this menu.

Table 119 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1	Select Yes to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the ZyXEL Device on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. None - The ZyXEL Device does not send or receive routing information on the subnet. Both - The ZyXEL Device sends and receives routing information on the subnet. In Only - The ZyXEL Device only receives routing information on the subnet. Out Only - The ZyXEL Device only sends routing information on the subnet.
Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information. RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information. RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.
Incoming protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).

Table 119 Menu 3.2.1: IP Alias Setup (continued)

FIELD	DESCRIPTION
Outgoing protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
IP Alias 2	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the ZyXEL Device on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. None - The ZyXEL Device does not send or receive routing information on the subnet. Both - The ZyXEL Device sends and receives routing information on the subnet. In Only - The ZyXEL Device only receives routing information on the subnet. Out Only - The ZyXEL Device only sends routing information on the subnet.
Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information. RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information. RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.
Incoming protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
Outgoing protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).

24.4 Wireless LAN Setup

Use this menu to configure basic wireless settings and wireless security. See [Chapter 6 on page 93](#) for background information. To open this menu, enter 5 in menu 3.

Figure 162 Menu 3.5: Wireless LAN Setup

Menu 3.5 - Wireless LAN Setup	
Enable Wireless LAN=	No
ESSID=	ZyXEL
Hide ESSID=	No
Channel ID=	CH06 2437MHz
WEP=	Disable
Key1=	N/A
Edit MAC Address Filter=	No

The ESSID in the SMT is the same as the SSID in the web configurator. The following table describes the labels in this menu.

Table 120 Menu 3.5: Wireless LAN Setup

FIELD	DESCRIPTION
Enable Wireless LAN	Select Yes to activate wireless LAN.
ESSID	Enter the name of the wireless network. The name is called the Extended Service Set IDentity (ESSID). Every wireless client in the same wireless network must use the same ESSID. Note: If you are using the wireless network to connect to the ZyXEL Device from a computer and you change this setting, you will lose your wireless connection when you press [ENTER] to confirm. You must change the wireless settings of your computer to match the ZyXEL Device's new settings.
Hide ESSID	Select this check box to hide the ESSID so a station cannot get the ESSID through scanning using a site survey tool.
Channel ID	Set the operating frequency or channel your wireless network uses. It should be at least five channels away from other wireless networks in the area.
WEP	Select the type of key you want to use. Disable - the wireless network does not use any encryption. 64-bit WEP - the wireless network uses a 64-bit WEP key. 128-bit WEP - the wireless network uses a 128-bit WEP key. A 128-bit WEP key is more secure than a 64-bit WEP key.
Key1	You can enter the key using printable ASCII characters or hexadecimal (0-9, A-F, a-f) characters. The ZyXEL Device and the wireless stations must use the same WEP key. If you selected a 64-bit WEP key, enter 5 printable ASCII characters or 10 hexadecimal characters. If you selected a 128-bit WEP key, enter 13 printable ASCII characters or 26 hexadecimal characters.
Edit MAC Address Filter	If you want to block or allow other devices to access the ZyXEL Device., press [SPACE BAR] to select Yes and press [ENTER]. Menu 3.5.1 appears.

24.5 WLAN MAC Address Filter

Use this menu to block or allow other devices to access the ZyXEL Device. See [Chapter 6 on page 93](#) for background information. To open this menu, select **Yes** in **Edit MAC Address Filter** in menu 3.5.

Figure 163 Menu 3.5.1: WLAN MAC Address Filter

Menu 3.5.1 - WLAN MAC Address Filter					
Active= No					
Filter Action= Allowed Association					

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

The following table describes the labels in this menu.

Table 121 Menu 3.5.1: WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	Select this to enable MAC address filtering.
Filter Action	Define the filter action for the MAC addresses in the table. Select Deny Association to stop these MAC addresses from accessing the ZyXEL Device. Other MAC address are allowed to access the ZyXEL Device. Select Allowed Association to allow these MAC addresses to access the ZyXEL Device. Other MAC addresses are not allowed to access the ZyXEL Device.
1-32	Enter the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in the format shown.

CHAPTER 25

Internet Access Setup

Use this menu to set up your Internet connection. See [Chapter 7 on page 119](#) and [Chapter 10 on page 137](#) for background information. To open this menu, enter 4 in the main menu.

Figure 164 Menu 4: Internet Access Setup

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPPoE

My Login= hello
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only
  
```

The following table describes the labels in this menu.

Table 122 Menu 4: Internet Access Setup

FIELD	DESCRIPTION
ISP's Name	Enter the name of the ISP.
Encapsulation	Select the type of encapsulation your ISP uses. If you select PPPoE and then save your changes, the ZyXEL Device asks you if you want to test the settings.
	The next fields are only available if your ISP uses PPPoE encapsulation.
My Login	Enter the user name provided by your ISP.
My Password	Enter the password provided by your ISP.
Retype to Confirm	Enter the password again.
Idle Timeout	Enter the number of seconds the ZyXEL Device should wait while there is no Internet traffic before it automatically disconnects from the ISP. Enter a time interval between 10 and 9999 seconds.
IP Address Assignment	Select Dynamic if your ISP did not give you a fixed (static) IP address. Select Static if your ISP gave you a fixed (static) IP address. The next three fields are not available if you select Dynamic .
IP Address	Enter the fixed (static) IP address provided by your ISP.
IP Subnet Mask	This field is not available if your ISP uses PPPoE encapsulation. Enter the subnet mask provided by your ISP.

Table 122 Menu 4: Internet Access Setup (continued)

FIELD	DESCRIPTION
Gateway IP Address	This field is not available if your ISP uses PPPoE encapsulation. Enter the IP address of the gateway provided by your ISP.
Network Address Translation	Select None if you do not want to use port forwarding, trigger ports, or NAT. Select SUA Only if you want to use one or more of these features and have only one WAN IP address for your ZyXEL Device. Select Full Feature if you want to use one or more of these features and have more than one public WAN IP address for your ZyXEL Device.

CHAPTER 26

Remote Node Setup

Use this menu to set up your Internet connection, input and output filter sets for the WAN port, advanced features for the WAN port, or a backup gateway.

26.1 Remote Node Profile

Use this menu to set up your Internet connection. See [Chapter 7 on page 119](#) and [Chapter 38 on page 347](#) for background information. To open this menu, enter 11 in the main menu.

Figure 165 Menu 11.1: Remote Node Profile

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes

Encapsulation= PPPoE              Edit IP= No
Telco Option:
Service Name=                     Allocated Budget (min)= 0
Outgoing:                          Period(hr)= 0
  My Login= hello                   Schedules=
  My Password= *****             Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

Session Options:
  Edit Filter Sets= No
  Idle Timeout(sec)= 100

Edit Traffic Redirect= No

```

The following table describes the labels in this menu.

Table 123 Menu 11.1: Remote Node Profile

FIELD	DESCRIPTION
Rem Node Name	Enter the name of the ISP.
Active	Select whether or not you want to use this Internet connection.
Encapsulation	Select the type of encapsulation your ISP uses. If you change this setting, you have to open menu 11.1.2 (Edit IP), update the settings, and save them before you can save the settings in this menu.
Service Name	Enter the service name provided by your ISP. Leave this field blank if your ISP did not provide one.

Table 123 Menu 11.1: Remote Node Profile (continued)

FIELD	DESCRIPTION
My Login	Enter the user name provided by your ISP.
My Password	Enter the password provided by your ISP.
Retype to Confirm	Enter the password again.
Authen	This field appears if you select PPPoE in the Encapsulation field. Select what type of authentication your ISP uses. Select CHAP/PAP if you want the ZyXEL Device to support both choices.
Route	This field displays the type of routing the ZyXEL Device uses.
Edit IP	If you want to set up the WAN IP address and advanced features for the WAN port, press [SPACE BAR] to select Yes and press [ENTER]. Menu 11.1.2 appears.
Telco Option	These fields appear if you select PPPoE in the Encapsulation field.
Allocated Budget(min)	Enter the maximum amount of time (in minutes) each call can last. Enter 0 if there is no limit. With Period , you can set a limit on the total outgoing call time of the ZyXEL Device within a certain period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.
Period(hr)	Enter how often (in hours) the Allocated Budget is reset. For example, if you can call for thirty minutes every hour, set the Allocated Budget to 30, and set this field to 1.
Schedules	Enter the schedule sets that apply to this connection.
Nailed-Up Connection	Select this if you want the ZyXEL Device to automatically connect to your ISP when it is turned on and to remain connected all the time. This is not recommended if you pay for your Internet connected based on the amount of time you are connected.
Session Options	
Edit Filter Sets	If you want to specify input and output filter sets for the WAN port, press [SPACE BAR] to select Yes and press [ENTER]. Menu 11.1.4 appears.
Idle Timeout(sec)	Enter the number of seconds the ZyXEL Device should wait while there is no Internet traffic before it automatically disconnects from the ISP. Enter a time interval between 10 and 9999 seconds.
Edit Traffic Redirect	If you want to set up a backup router, if you have one, in case the ZyXEL Device cannot access the Internet, press [SPACE BAR] to select Yes and press [ENTER]. Menu 11.1.5 appears.

26.2 Remote Node Network Layer Options

Use this menu to set up the WAN IP address and advanced features for the WAN port. See [Chapter 7 on page 119](#) and [Chapter 10 on page 137](#) for background information. To open this menu, select **Yes** in **Edit IP** in menu 11.1.

Figure 166 Menu 11.1.2: Remote Node Network Layer Options

```

Menu 11.1.2 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
Rem IP Addr= N/A
Rem Subnet Mask= N/A
My WAN Addr= N/A

Network Address Translation= SUA Only
Metric= 1
Private= N/A
RIP Direction= Both
    Version= RIP-1
Multicast= None
    
```

The following table describes the labels in this menu.

Table 124 Menu 11.1.2: Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	Select Dynamic if your ISP did not give you a fixed (static) IP address. Select Static if your ISP gave you a fixed (static) IP address. The next three fields are not available if you select Dynamic .
	These fields appear if you selected Ethernet in Encapsulation in menu 11.
IP Address	Enter the fixed (static) IP address provided by your ISP.
IP Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Addr	Enter the IP address of the gateway provided by your ISP.
	These fields appear if you selected PPPoE in Encapsulation in menu 11.
Rem IP Addr	Enter the IP address of the remote (peer) computer to which the ZyXEL Device connects.
Rem Subnet Mask	Enter the subnet mask of the remote (peer) computer to which the ZyXEL Device connects.
My WAN Addr	Enter the fixed (static) IP address provided by your ISP.
Network Address Translation	Select None if you do not want to use port forwarding, trigger ports, or NAT. Select SUA Only if you want to use one or more of these features and have only one WAN IP address for your ZyXEL Device. Select Full Feature if you want to use one or more of these features and have more than one public WAN IP address for your ZyXEL Device.
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".

Table 124 Menu 11.1.2: Remote Node Network Layer Options (continued)

FIELD	DESCRIPTION
Private	This field is related to RIP. This field determines whether or not the ZyXEL Device includes the route to this remote node in its RIP broadcasts. If you select Yes , this route is not included in RIP broadcast. If you select No , the route to this remote node is propagated to other hosts through RIP broadcasts. Usually, you should keep the default value.
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives through this connection. None - The ZyXEL Device does not send or receive routing information through this connection. Both - The ZyXEL Device sends and receives routing information through this connection. In Only - The ZyXEL Device only receives routing information through this connection. Out Only - The ZyXEL Device only sends routing information through this connection.
Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information. RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information. RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.
Multicast	You do not have to enable multicasting to use RIP-2M . (See RIP Version .) Select which version of IGMP the ZyXEL Device uses to support multicasting on this port. Multicasting only sends packets to some computers and is an alternative to unicasting (sending packets to one computer) and broadcasting (sending packets to every computer). None - The ZyXEL Device does not support multicasting. IGMP-v1 - The ZyXEL Device supports IGMP version 1. IGMP-v2 - The ZyXEL Device supports IGMP version 2. Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers have to support the same version of IGMP.

26.3 Remote Node Filter

Use this menu to specify input and output filter sets for the WAN port. See [Chapter 30 on page 287](#) for background information. To open this menu, select **Yes** in **Edit Filter Sets** in menu 11.1.

Figure 167 Menu 11.1.4: Remote Node Filter

```

Menu 11.1.4 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Call Filter Sets:
  protocol filters=
  device filters=

```

The following table describes the labels in this menu.

Table 125 Menu 11.1.4: Remote Node Filter

FIELD	DESCRIPTION
Input Filter Sets	
protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
device filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
Output Filter Sets	
protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
device filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
Call Filter Sets	These fields appear if you selected PPPoE in Encapsulation in menu 11.
protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
device filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).

26.4 Traffic Redirect Setup

Use this menu to set up a backup router, if you have one, in case the ZyXEL Device cannot access the Internet. See [Chapter 7 on page 119](#) for background information. To open this menu, select **Yes** in **Edit Traffic Redirect** in menu 11.1.

Figure 168 Menu 11.1.5: Traffic Redirect Setup

```

Menu 11.1.5 - Traffic Redirect Setup

Active= No
Configuration:
Backup Gateway IP Address= 0.0.0.0
Metric= 14
Check WAN IP Address= 0.0.0.0
Fail Tolerance= 3
Period(sec)= 5
Timeout(sec)= 3

```

The following table describes the labels in this menu.

Table 126 Menu 11.1.5: Traffic Redirect Setup

FIELD	DESCRIPTION
Active	Select this to set up a backup gateway in case the default gateway is not available. (For example, this might happen if the Internet connection goes down.) Clear this if you do not have a backup gateway.
Configuration	
Backup Gateway IP Address	Enter the IP address of the backup gateway. The ZyXEL Device automatically uses this gateway if the default gateway is not available anymore.
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". A backup gateway usually has a higher cost than the default gateway so that the ZyXEL Device uses the default gateway as long as it is available.
Check WAN IP Address	Enter the IP address of a reliable nearby computer the ZyXEL Device uses to test whether or not the default gateway is available anymore. For example, use one of your ISP's DNS server addresses. If you enter 0.0.0.0, the test fails every time.
Fail Tolerance	Enter the number of consecutive times the ZyXEL Device may attempt and fail to find the reliable nearby computer at Check WAN IP Address before it starts using the backup gateway. 2-5 are typical choices.
Period(sec)	Enter the number of seconds between attempts to find the reliable nearby computer at Check WAN IP Address . 5-60 are typical choices.
Timeout(sec)	Enter the number of seconds the ZyXEL Device waits for a response from the reliable nearby computer at Check WAN IP Address before the attempt is a failure. 3-50 are typical choices, but this number should be less than the Period .

CHAPTER 27

Static Routing Setup

Use this menu to look at and configure IP static routes.

27.1 IP Static Route Setup

Use this menu to look at IP static routes. See [Chapter 14 on page 193](#) for background information. To open this menu, enter 12 in the main menu.

Figure 169 Menu 12: IP Static Route Setup

```

Menu 12 - IP Static Route Setup

1. Reserved      16. _____  31. _____  46. _____
2. _____    17. _____  32. _____  47. _____
3. _____    18. _____  33. _____  48. _____
4. _____    19. _____  34. _____  49. _____
5. _____    20. _____  35. _____  50. _____
6. _____    21. _____  36. _____
7. _____    22. _____  37. _____
8. _____    23. _____  38. _____
9. _____    24. _____  39. _____
10. _____   25. _____  40. _____
11. _____   26. _____  41. _____
12. _____   27. _____  42. _____
13. _____   28. _____  43. _____
14. _____   29. _____  44. _____
15. _____   30. _____  45. _____

Enter selection number:

```

The following table describes the labels in this menu.

Table 127 Menu 12: IP Static Route Setup

FIELD	DESCRIPTION
1-50	This field shows the beginning of the name of each IP static route.
Enter selection number	If you want to configure an IP static route, enter the number of the static route, and press [ENTER]. Menu 12.1 appears. You cannot edit the first static route, which is the default route for the ZyXEL Device.

27.2 Edit IP Static Route

Use this menu to configure IP static routes. See [Chapter 14 on page 193](#) for background information. To open this menu, enter an IP static route number in **Enter selection number** in menu 12.

Figure 170 Menu 12.1: Edit IP Static Route

```

Menu 12.1 - Edit IP Static Route

Route #: 2
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

```

The following table describes the labels in this menu.

Table 128 Menu 12.1: Edit IP Static Route

FIELD	DESCRIPTION
Route	This field displays the number of the static route.
Route Name	Enter the name of the static route. If you leave this field blank, you can delete the static route by pressing [ENTER].
Active	Select this if you want the static route to be used. Clear this if you do not want the static route to be used.
Destination IP Address	Enter one of the destination IP addresses that this static route affects.
IP Subnet Mask	Enter the subnet mask that defines the range of destination IP addresses that this static route affects. If this static route affects only one IP address, enter 255.255.255.255.
Gateway IP Address	Enter the IP address of the gateway to which the ZyXEL Device should send packets for the specified Destination . The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	This field is related to RIP. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the metric, the lower the "cost". RIP uses hop count as the measurement of cost, where 1 is for a directly-connected network. The metric must be 1-15; if you use a value higher than 15, the routers assume the link is down. Usually, you should keep the default value.
Private	Select this if you do not want the ZyXEL Device to tell other routers about this static route. For example, you might select this if the static route is in your LAN. Clear this if you want the ZyXEL Device to tell other routers about this static route.

CHAPTER 28

Dial-in User Setup

Use this menu to look at and configure local user profiles on the ZyXEL Device.

28.1 Dial-in User Setup

Use this menu to look at local user profiles on the ZyXEL Device. See [Chapter 6 on page 93](#) for background information. To open this menu, enter 14 in the main menu.

Figure 171 Menu 14: Dial-in User Setup

Menu 14 - Dial-in User Setup

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

Enter Menu Selection Number:

The following table describes the labels in this menu.

Table 129 Menu 14: Dial-in User Setup

FIELD	DESCRIPTION
1-32	This field shows the beginning of the user name of each local user profile.
Enter Menu Selection Number	If you want to configure a local user profile, enter the number of the profile, and press [ENTER]. Menu 14.1 appears.

28.2 Edit Dial-in User

Use this menu to configure local user profiles on the ZyXEL Device. See [Chapter 6 on page 93](#) for background information. To open this menu, enter a local user profile number in **Enter Menu Selection Number** in menu 14.

Figure 172 Menu 14.1: Edit Dial-in User

Menu 14.1 - Edit Dial-in User User Name= ? Active= No Password= ?
--

The following table describes the labels in this menu.

Table 130 Menu 14.1: Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case-sensitive.
Active	Press [SPACE BAR] to select Yes and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile. This field is case-sensitive.

CHAPTER 29

NAT Setup

Use this menu to configure address mapping, port forwarding, and trigger ports.

29.1 Address Mapping Sets

Use this menu to select which address mapping set you want to configure. See [Chapter 10 on page 137](#) for background information. To open this menu, enter 1 in menu 15.

Figure 173 Menu 15.1: Address Mapping Sets

Menu 15.1 - Address Mapping Sets	
1.	ACL Default Set
255.	SUA (read only)

You cannot create The following table describes the labels in this menu.

Table 131 Menu 15.1: Address Mapping Sets

FIELD	DESCRIPTION
1	Select this if you want to configure NAT address mapping rules. Menu 15.1.1 appears.
255	Select this if you want to look at SUA address mapping rules. Menu 15.1.255 appears. Menu 15.1.255 is similar to menu 15.1.1, except there are no fields which allow you to edit the rules.

29.2 Address Mapping Rules

Use this menu to look at network address translation mapping rules. See [Chapter 10 on page 137](#) for background information. To open this menu, select one of the address mapping sets in menu 15.1.

Figure 174 Menu 15.1.1: Address Mapping Rules

```

Menu 15.1.1 - Address Mapping Rules

Set Name= ACL Default Set

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

Action= None          Select Rule= N/A
    
```

The following table describes the labels in this menu.

Table 132 Menu 15.1.1: Address Mapping Rules

FIELD	DESCRIPTION
Set Name	Enter a descriptive name for the NAT mapping rules.
Idx	This is the rule index number.
Local Start IP Local End IP	This is the range of IP addresses on the LAN port. Local Start IP is N/A for Server port mapping. Local End IP is N/A for One-to-one and Server mapping types.
Global Start IP Global End IP	This is the corresponding range of IP addresses on the WAN port. Global Start IP should be 0.0.0.0 if both of the following conditions are satisfied. <ul style="list-style-type: none"> Your ISP assigns the IP address of your WAN port. The rule is a Many-to-One or Server rule. Global End IP is N/A for One-to-one , Many-to-One and Server mapping types.

Table 132 Menu 15.1.1: Address Mapping Rules (continued)

FIELD	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>
Action Select Rule	In the Action field, press the [SPACEBAR] to select what change you would like to make. For some actions, enter the rule number in the Select Rule field to specify on which rule you would like to apply the action.

29.3 Address Mapping Rule

Use this menu to configure network address translation mapping rules. See [Chapter 10 on page 137](#) for background information. To open this menu, select one of the address mapping rules in menu 15.1.1.

Figure 175 Menu 15.1.1.1: Address Mapping Rule

Menu 15.1.1.1 Address Mapping Rule
Type= One-to-One
Local IP:
Start=
End = N/A
Global IP:
Start=
End = N/A

The following table describes the labels in this menu.

Table 133 Menu 15.1.1.1: Address Mapping Rule

FIELD	DESCRIPTION
Type	<p>Choose the port mapping type from one of the following.</p> <ul style="list-style-type: none"> • 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. • 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. • Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. • Many-to-Many No Overload: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. • Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local IP: Start End	<p>Enter the range of IP addresses on the LAN port.</p> <p>Local Start IP is N/A for Server port mapping.</p> <p>Local End IP is N/A for One-to-one and Server mapping types.</p> <p>To create a rule for all LAN IP addresses, set Local Start IP to 0.0.0.0 and Local End IP to 255.255.255.255.</p>
Global IP: Start End	<p>This is the corresponding range of IP addresses on the WAN port.</p> <p>Global Start IP should be 0.0.0.0 if both of the following conditions are satisfied.</p> <ul style="list-style-type: none"> • Your ISP assigns the IP address of your WAN port. • The rule is a Many-to-One or Server rule. <p>Global End IP is N/A for One-to-one, Many-to-One and Server mapping types.</p>

29.4 NAT Server Setup

Use this menu to look at servers for which you have configured port forwarding rules. See [Chapter 10 on page 137](#) for background information. To open this menu, enter 2 in menu 15.

Figure 176 Menu 15.2: NAT Server Setup

Menu 15.2 - NAT Server Setup					
Default Server: 0.0.0.0					
Rule	Act.	Start Port	End Port	IP Address	
001	No	0	0	0.0.0.0	
002	No	0	0	0.0.0.0	
003	No	0	0	0.0.0.0	
004	No	0	0	0.0.0.0	
005	No	0	0	0.0.0.0	
006	No	0	0	0.0.0.0	
007	No	0	0	0.0.0.0	
008	No	0	0	0.0.0.0	
009	No	0	0	0.0.0.0	
010	No	0	0	0.0.0.0	
Select Command= None			Select Rule= N/A		

The following table describes the labels in this menu.

Table 134 Menu 15.2: NAT Server Setup

FIELD	DESCRIPTION
Default Server	Enter the IP address of the server to which the ZyXEL Device should forward packets for ports that are not specified in the section below or in menu 24.11 (remote management). Enter 0.0.0.0 if you want the ZyXEL Device to discard these packets instead.
Rule	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 active rule in order, and it only follows the first one that applies.
Act.	This field displays whether or not this rule is active.
Start Port	This field displays the beginning of the range of port numbers forwarded by this rule.
End Port	This field displays the end of the range of port numbers forwarded by this rule. If it is the same as the Start Port , only one port number is forwarded.
IP Address	This field displays the IP address of the server to which packet for the selected port(s) are forwarded.
Select Command Select Rule	In the Select Command field, press the [SPACEBAR] to select what change you would like to make. For some actions, enter the rule number in the Select Rule field to specify on which rule you would like to apply the action.

29.5 NAT Server Configuration

Use this menu to configure port forwarding rules for servers behind the ZyXEL Device. See [Chapter 10 on page 137](#) for background information. To open this menu, select one of the port forwarding rules in menu 15.2.

Figure 177 Menu 15.2.1: NAT Server Configuration

```

15.2.1 - NAT Server Configuration

Wan= 1                               Index= 1
-----

Name=

Active= No

Start port= 0                         End port= 0

IP Address= 0.0.0.0

```

The following table describes the labels in this menu.

Table 135 Menu 15.2.1: NAT Server Configuration

FIELD	DESCRIPTION
Wan	This field indicates that the rule applies to packets from the WAN.
Index	This field shows the corresponding rule number. The sequence is important, however. The ZyXEL Device checks each active rule in order, and it only follows the first one that applies.
Name	Enter a name to identify this rule. You can use 1 - 31 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Active	Select this to enable this rule. Clear this to disable this rule.
Start port End port	Enter the port number or range of port numbers you want to forward to the specified server. To forward one port number, enter the port number in the Start port and End port fields. To forward a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start port field enter the port number at the end of the range in the End port field.
IP Address	Enter the IP address of the server to which to forward packets for the selected port number(s). This server is usually on the LAN.

29.6 Trigger Port Setup

Use this menu to change your ZyXEL Device's port triggering settings. See [Chapter 10 on page 137](#) for background information. To open this menu, enter 3 in menu 15.

Figure 178 Menu 15.3: Trigger Port Setup

Menu 15.3 - Trigger Port Setup					
Rule	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1.		0	0	0	0
2.		0	0	0	0
3.		0	0	0	0
4.		0	0	0	0
5.		0	0	0	0
6.		0	0	0	0
7.		0	0	0	0
8.		0	0	0	0
9.		0	0	0	0
10.		0	0	0	0
11.		0	0	0	0
12.		0	0	0	0

The following table describes the labels in this menu.

Table 136 Menu 15.3: Trigger Port Setup

FIELD	DESCRIPTION
Name	Enter a name to identify this rule. You can use 1 - 15 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Incoming	
Start Port End Port	Enter the incoming port number or range of port numbers you want to forward to the IP address the ZyXEL Device records. To forward one port number, enter the port number in the Start Port and End Port fields. To forward a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start Port field enter the port number at the end of the range in the End Port field. If you want to delete this rule, enter zero in the Start Port and End Port fields.
Trigger	
Start Port End Port	Enter the outgoing port number or range of port numbers that makes the ZyXEL Device record the source IP address and assign it to the selected incoming port number(s). To select one port number, enter the port number in the Start Port and End Port fields. To select a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start Port field enter the port number at the end of the range in the End Port field. If you want to delete this rule, enter zero in the Start Port and End Port fields.

CHAPTER 30

Filter Setup

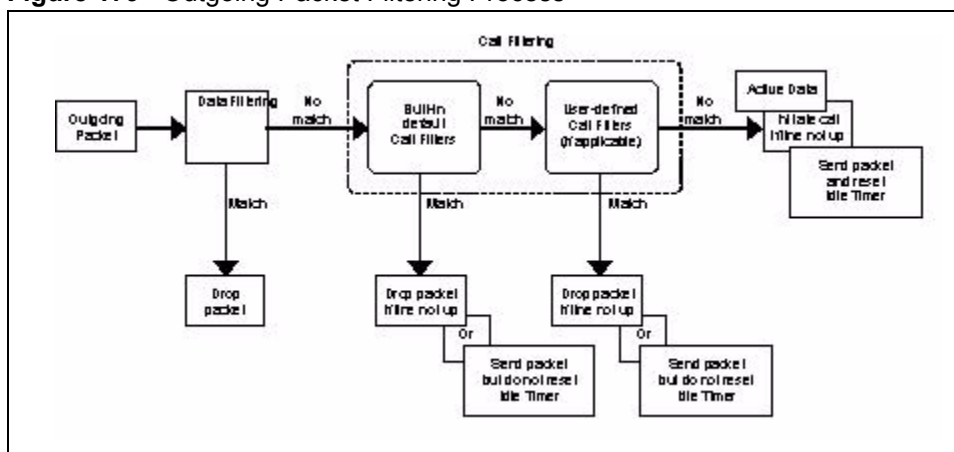
This chapter shows you how to create and apply filters.

30.1 Introduction to Filters

Your ZyXEL Device uses filters to decide whether 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 the 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 LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

Figure 179 Outgoing Packet Filtering Process



For incoming packets, your ZyXEL Device applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

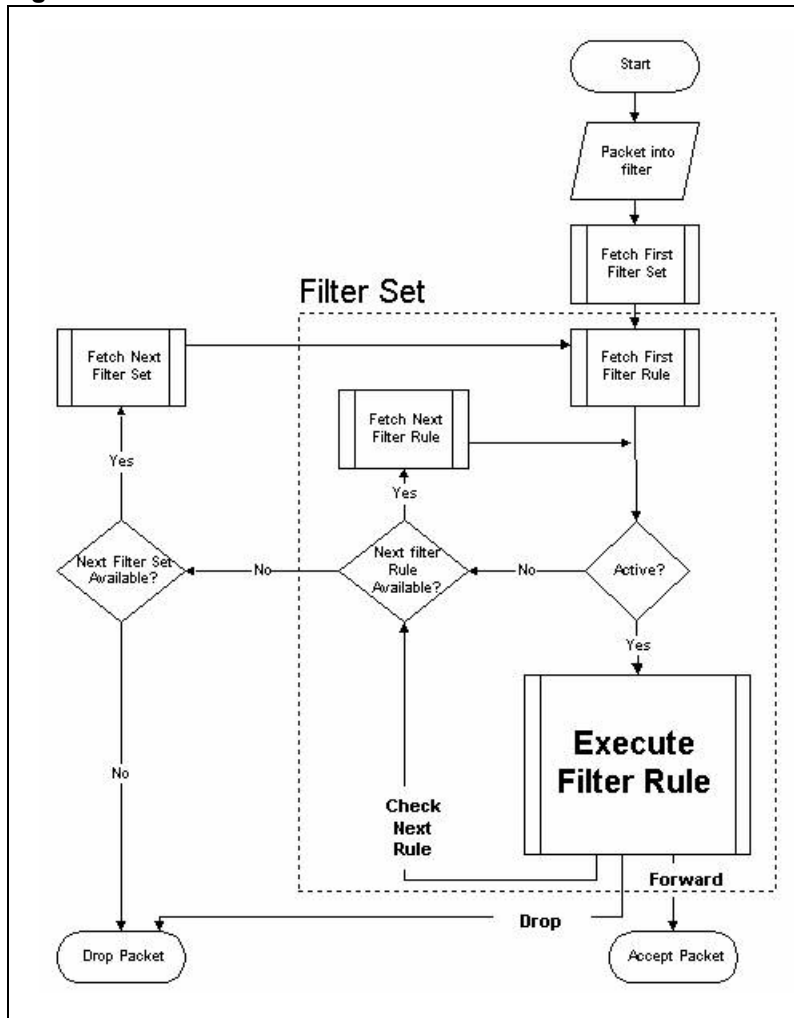
30.1.1 The Filter Structure of the ZyXEL Device

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyXEL Device allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. 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. See also [Figure 185 on page 295](#) for the logic flow when executing an IP filter.

Figure 180 Filter Rule Process



You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

30.2 Configuring a Filter Set

The ZyXEL Device includes filtering for NetBIOS over TCP/IP packets and IGMP by default. To configure another filter set, follow the procedure below.

- 1 Enter 21 in the main menu to open menu 21.

Figure 181 Menu 21: Filter and Firewall Setup

```

Menu 21 - Filter and Firewall Setup

1. Filter Setup
2. Firewall Setup
    
```

2 Enter 1 to bring up the following menu.

Figure 182 Menu 21.1: Filter Set Configuration

```

Menu 21.1 - Filter Set Configuration

Filter                               Filter
Set #                               Set #
-----                               -----
1                                     7
2   NetBIOS_WAN                       8
3   NetBIOS_LAN                       9
4   IGMP                               10
5                                     11
6                                     12

Enter Filter Set Number to Configure= 0

Edit Comments= N/A
    
```

Select the filter set you wish to configure (1-12) and press [ENTER].

Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

Figure 183 Menu 21.1.1: Filter Rules Summary

Menu 21.1.1 - Filter Rules Summary							
#	A	Type	Filter Rules			M m n	
1	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=137	N D N
2	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=138	N D N
3	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=139	N D N
4	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=137	N D N
5	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=138	N D N
6	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=139	N D F

Enter Filter Rule Number (1-6) to Configure:

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 137 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 138 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol

Table 138 Rule Abbreviations Used (continued)

ABBREVIATION	DESCRIPTION
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

30.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyXEL Device will warn you and will not allow you to save.

30.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next

Figure 184 Menu 21.1.1.1 TCP/IP Filter Rule.

```

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr=
                IP Mask=
                Port #=
                Port # Comp= None
Source: IP Addr=
         IP Mask=
         Port #=
         Port # Comp= None
TCP Estab= N/A
More= No          Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule
    
```

The following table describes how to configure your TCP/IP filter rule.

Table 139 TCP/IP Filter Rule

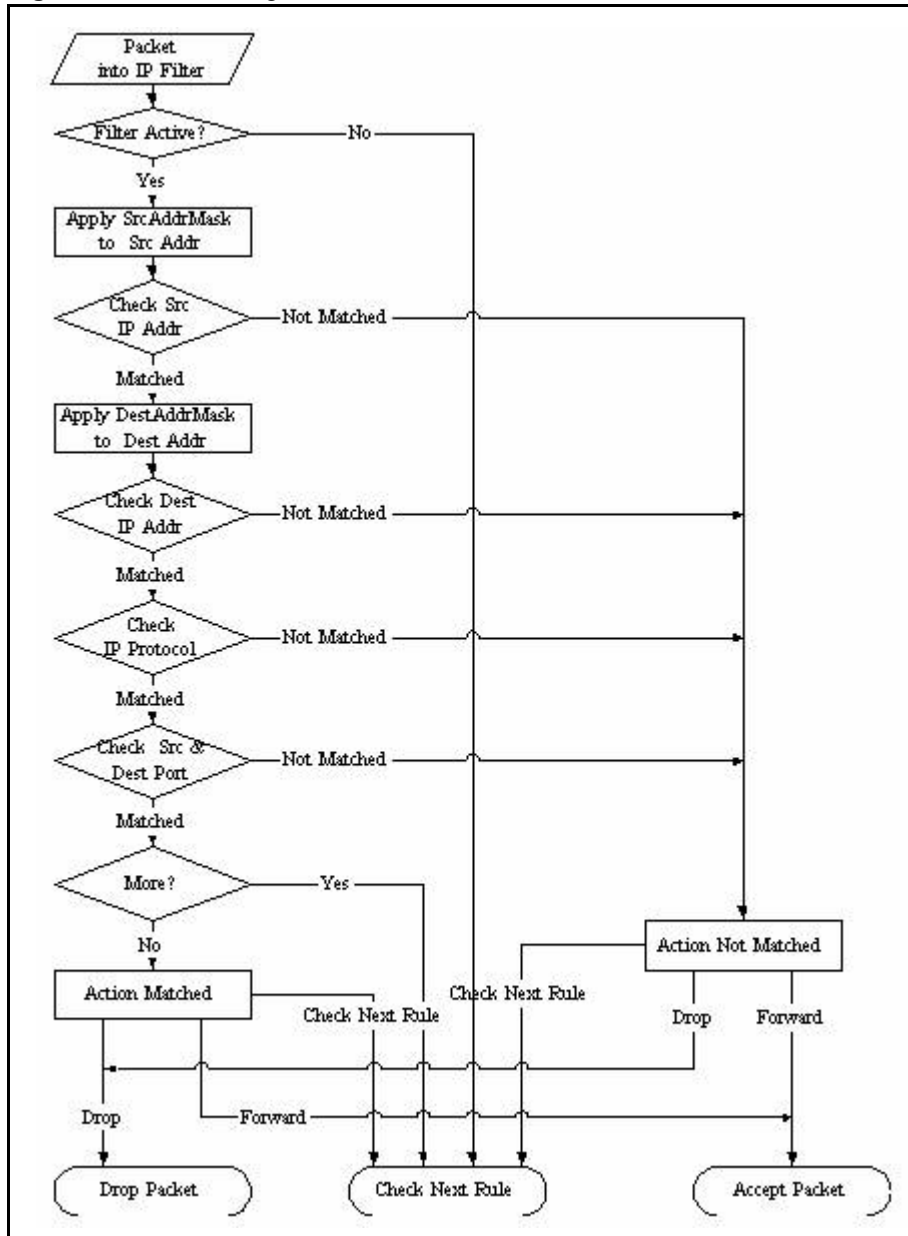
FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule coordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	Generic Filter Rule TCP/IP Filter Rule
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate the filter rule or No to deactivate it.	Yes No
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	Press [SPACE BAR] and then [ENTER] to select Yes to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.	Yes No
Destination		
IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the Destination: IP Addr .	0.0.0.0
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535

Table 139 TCP/IP Filter Rule (continued)

FIELD	DESCRIPTION	OPTIONS
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in Destination: Port # .	None Less Greater Equal Not Equal
Source		
IP Addr	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the Source: IP Addr .	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in Source: Port # .	None Less Greater Equal Not Equal
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select Yes , to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if No , it is ignored.	Yes No
More	Press [SPACE BAR] and then [ENTER] to select Yes or No . If Yes , a matching packet is passed to the next filter rule before an action is taken; if No , the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A .	Yes No
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: None – No packets will be logged. Action Matched - Only packets that match the rule parameters will be logged. Action Not Matched - Only packets that do not match the rule parameters will be logged. Both – All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	Check Next Rule Forward Drop
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	Check Next Rule Forward Drop

The following figure illustrates the logic flow of an IP filter.

Figure 185 Executing an IP Filter



30.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyXEL Device treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyXEL Device applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.1.1 and press [ENTER] to open Generic Filter Rule, as shown below.

Figure 186 Menu 21.1.1.1 Generic Filter Rule

```
Menu 21.1.4.1 - Generic Filter Rule

Filter #: 4,1
Filter Type= Generic Filter Rule
Active= Yes
Offset= 0
Length= 3
Mask= ffffff
Value= 01005e
More= No           Log= None
Action Matched= Drop
Action Not Matched= Forward
```

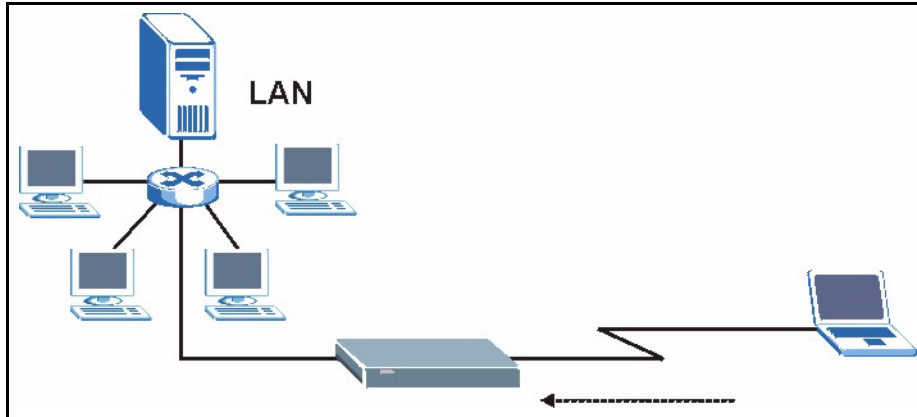
The following table describes the fields in the Generic Filter Rule menu.

Table 140 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule coordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	Generic Filter Rule TCP/IP Filter Rule
Active	Select Yes to turn on the filter rule or No to turn it off.	Yes / No
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0-255
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0-8
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	
More	If Yes , a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be No .	Yes No
Log	Select the logging option from the following: None - No packets will be logged. Action Matched - Only packets that match the rule parameters will be logged. Action Not Matched - Only packets that do not match the rule parameters will be logged. Both - All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Select the action for a packet matching the rule.	Check Next Rule Forward Drop
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule Forward Drop

30.3 Example Filter

Let's look at an example to block outside users from accessing the ZyXEL Device via telnet.

Figure 187 Telnet Filter Example

- 1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- 2 Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
- 3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
- 4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- 5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**
- 6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Figure 188 Example Filter: Menu 21.1.3.1

```

Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 23
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None
TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

- Select **Yes** from the **Active** field to activate this rule.
- **6** is the **TCP IP Protocol**.

- The **Port #** for the telnet service (TCP protocol) is 23. See RFC 1060 for port numbers of well-known services.
- Select **Equal** from the **Port # Comp** field as you are looking for packets going to port 23 only.
- Select **Drop** in the **Action Matched** field so that the packet will be dropped if its destination is the telnet port.
- Select **Forward** from the **Action Not Matched** field so that the packet will be forwarded if its destination is not the telnet port.
- Press [SPACE BAR] and then [ENTER] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Figure 189 Example Filter Rules Summary: Menu 21.1.3

Menu 21.1.3 - Filter Rules Summary			
#	A	Type	Filter Rules
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23
2	N		
3	N		
4	N		
5	N		
6	N		

Enter Filter Rule Number (1-6) to Configure:

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP, Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

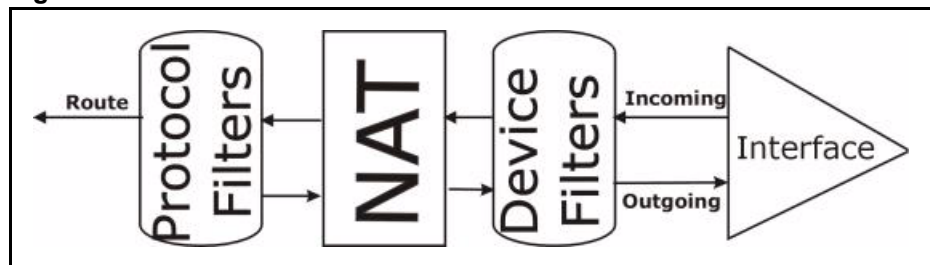
After you've created the filter set, you must apply it.

- 1 Enter 11 from the main menu to go to menu 11.
- 2 Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
- 3 This brings you to menu 11.5. Apply a filter set (our example filter set 3).
- 4 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

30.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyXEL Device applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyXEL Device is receiving and sending the packets; i.e., the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 190 Protocol and Device Filter Sets



30.5 Firewall Versus Filters

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

30.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The ZyXEL Device already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Note: If you do not activate the firewall, it is advisable to apply filters

30.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyXEL Device and output filter sets filter outgoing traffic from the ZyXEL Device. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 191 Filtering LAN Traffic

```
Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=

Output Filter Sets:
  protocol filters=
  device filters=

Press ENTER to Confirm or ESC to Cancel:
```

30.6.2 Applying Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The ZyXEL Device already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Figure 192 Filtering Remote Node Traffic

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=

Output Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

Use this menu to set up your Internet connection, input and output filter sets for the WAN port, advanced features for the WAN port, or a backup gateway.

30.7 Remote Node Profile

Use this menu to set up your Internet connection. See [Chapter 7 on page 119](#) for background information. To open this menu, enter 11 in the main menu.

Figure 193 Menu 11.1: Remote Node Profile

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes

Encapsulation= PPPoE             Edit IP= No
Telco Option:
Service Name=                    Allocated Budget(min)= 0
Outgoing:                         Period(hr)= 0
  My Login= hello                 Schedules=
  My Password= *****           Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

Session Options:
  Edit Filter Sets= No
  Idle Timeout(sec)= 100

Edit Traffic Redirect= No

```

The following table describes the labels in this menu.

Table 141 Menu 11.1: Remote Node Profile

FIELD	DESCRIPTION
Rem Node Name	Enter the name of the ISP.
Active	Select whether or not you want to use this Internet connection.
Encapsulation	Select the type of encapsulation your ISP uses.
Service Name	Enter the service name provided by your ISP. Leave this field blank if your ISP did not provide one.
My Login	Enter the user name provided by your ISP.
My Password	Enter the password provided by your ISP.
Retype to Confirm	Enter the password again.
Authen	This field appears if you select PPPoE in the Encapsulation field. Select what type of authentication your ISP uses. Select CHAP/PAP if you want the ZyXEL Device to support both choices.
Route	This field displays the type of routing the ZyXEL Device uses.
Edit IP	If you want to set up the WAN IP address and advanced features for the WAN port, press [SPACE BAR] to select Yes and press [ENTER]. Menu 11.1.2 appears.
Telco Option	These fields appear if you select PPPoE in the Encapsulation field.
Allocated Budget(min)	Enter the maximum amount of time (in minutes) each call can last. Enter 0 if there is no limit.
Period(hr)	Enter how often (in hours) the Allocated Budget is reset. For example, if you can call for thirty minutes every hour, set the Allocated Budget to 30, and set this field to 1.
Schedules	Enter the schedule sets that apply to this connection.

Table 141 Menu 11.1: Remote Node Profile (continued)

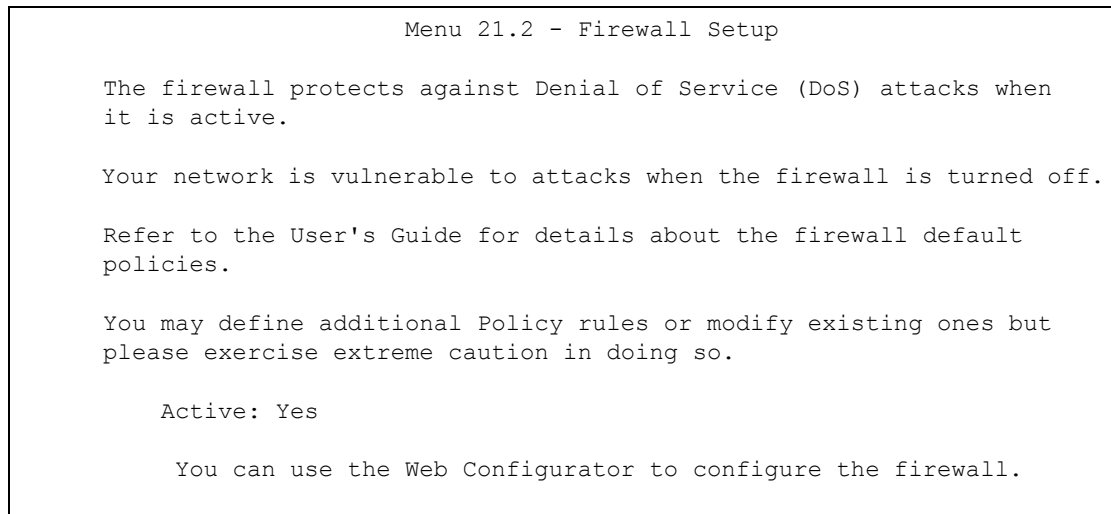
FIELD	DESCRIPTION
Nailed-Up Connection	Select this if you want the ZyXEL Device to automatically connect to your ISP when it is turned on and to remain connected all the time. This is not recommended if you pay for your Internet connected based on the amount of time you are connected.
Session Options	
Edit Filter Sets	If you want to specify input and output filter sets for the WAN port, press [SPACE BAR] to select Yes and press [ENTER]. Menu 11.1.4 appears.
Idle Timeout(sec)	Enter the number of seconds the ZyXEL Device should wait while there is no Internet traffic before it automatically disconnects from the ISP. Enter a time interval between 10 and 9999 seconds.
Edit Traffic Redirect	If you want to set up a backup router, if you have one, in case the ZyXEL Device cannot access the Internet, press [SPACE BAR] to select Yes and press [ENTER]. Menu 11.1.5 appears.

CHAPTER 31

Firewall Setup

Use this menu to activate or deactivate the firewall. See [Chapter 11 on page 147](#) for background information. To open this menu, enter 2 in menu 21.

Figure 194 Menu 21.2: Firewall Setup



Select **Yes** to activate the firewall. Select **No** to deactivate the firewall.

CHAPTER 32

SNMP Configuration

Use this menu to configure your ZyXEL Device's settings for Simple Network Management Protocol (SNMP) management. See [Chapter 16 on page 205](#) for background information. To open this menu, enter 22 in the main menu.

Figure 195 Menu 22: SNMP Configuration

```

Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
  Trap:
    Community= public
    Destination= 0.0.0.0

```

The following table describes the labels in this menu.

Table 142 Menu 22: SNMP Configuration

FIELD	DESCRIPTION
Get Community	Enter the password for incoming Get requests and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the password for incoming Set requests from the management station. The default is public and allows all requests.
Trusted Host	Enter an IP address to only allow the computer with this IP address to access the ZyXEL Device using this service. Enter 0.0.0.0 to allow any computer to access the ZyXEL Device using this service. This is the same field you can set up in menu 24.11.
Trap	
Community	Type 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 which send SNMP traps.

CHAPTER 33

System Security

Use this menu to configure the administrator password and to configure wireless authentication for the ZyXEL Device.

33.1 Change Password

Use this menu to change the administrator password for the ZyXEL Device. This is the same password used to access the web configurator. To open this menu, enter 1 in menu 23.

Figure 196 Menu 23.1: System Security - Change Password

<pre> Menu 23.1 - System Security - Change Password Old Password= ? New Password= ? Retype to confirm= ? </pre>
--

The following table describes the labels in this menu.

Table 143 Menu 23.1: System Security - Change Password

FIELD	DESCRIPTION
Old Password	Enter the current administrator password for the ZyXEL Device.
New Password	Enter the new administrator password for the ZyXEL Device.
Retype to confirm	Enter the new administrator password again.

33.2 RADIUS Server

Use this menu to configure a RADIUS server to use for wireless user authentication. See [Chapter 6 on page 93](#) for background information. To open this menu, enter 2 in menu 23.

Figure 197 Menu 23.2: System Security - RADIUS Server

```

Menu 23.2 - System Security - RADIUS Server

Authentication Server:
  Active= Yes
  Server Address= 192.168.1.100
  Port #= 1812
  Shared Secret= *****

Accounting Server:
  Active= No
  Server Address= 0.0.0.0
  Port #= 1813
  Shared Secret= *****

```

The following table describes the labels in this menu.

Table 144 Menu 23.2: System Security - RADIUS Server

FIELD	DESCRIPTION
Authentication Server	
Active	Select this to enable wireless authentication using a RADIUS server.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port #	Enter the port number of the external authentication server. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Enter a password (up to 31 alphanumeric characters) to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server. The key is not sent over the network.
Accounting Server	These settings are optional.
Active	Select this to enable user accounting through an external authentication server.
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port #	Enter the port number of the external accounting server. You need not change this value unless your network administrator instructs you to do so.
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. The key is not sent over the network.

33.3 IEEE802.1x

Use this menu to configure IEEE 802.1x wireless authentication for the ZyXEL Device. See [Chapter 6 on page 93](#) for background information. To open this menu, enter 4 in menu 23.

Figure 198 Menu 23.4: System Security - IEEE802.1x

Menu 23.4 - System Security - IEEE802.1x	
Wireless Port Control=	No Authentication Required
ReAuthentication Timer (in second)=	N/A
Idle Timeout (in second)=	N/A
Key Management Protocol=	N/A
Dynamic WEP Key Exchange=	N/A
PSK =	N/A
WPA Mixed Mode=	N/A
WPA Broadcast/Multicast Key Update Timer=	N/A
Authentication Databases=	N/A

The following table describes the labels in this menu.

Table 145 Menu 23.4: System Security - IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	Select No Authentication Required to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting. Select Authentication Required to require wireless stations to enter usernames and passwords before access to the wired network is allowed. Select No Access Allowed to deny all wireless stations access to the wired network. The rest of the fields are not available when you select No Authentication Required or No Access Allowed .
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to enter the username and password again before it can use the wireless network again. Some wireless clients can do this automatically; some wireless clients cannot, in which case the user has to enter the information again. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. Enter a time interval between 10 and 9999 seconds. 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 minimize the number of delays caused by logging in again.
Key Management Protocol	Select the type of IEEE 802.1x security you want to use.
Dynamic WEP Key Exchange	This field is enabled if the Key Management Protocol is 802.1x . Select the length of the WEP keys the ZyXEL Device generates. The longer the key, the stronger the security, but also the more processing is required.

Table 145 Menu 23.4: System Security - IEEE802.1x (continued)

FIELD	DESCRIPTION
PSK	This field is enabled if the Key Management Protocol is WPA-PSK or WPA2-PSK . Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). The key is case-sensitive.
WPA Mixed Mode	This field is enabled if the Key Management Protocol is WPA , WPA2 , or WPA2-PSK . Select this to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
WPA Broadcast/ Multicast Key Update Timer	This is the rate at which the ZyXEL Device sends a new group key to all clients. This process changes the WEP key on a regular basis. Enter a time interval between 10 and 9999 seconds.
Authentication Databases	This field is enabled if the Key Management Protocol is 802.1x . If the Key Management Protocol is WPA or WPA2 , this field is read-only and shows RADIUS Only . Select which database(s) the ZyXEL Device uses to authenticate wireless stations. The choices are Local User Database Only ; RADIUS Only ; Local first, then RADIUS ; and RADIUS first, then Local .

CHAPTER 34

System Maintenance 24.1 - 24.4

This chapter covers menus 24.1 through 24.4. Use these menus to get a variety of system information and to perform system diagnostics.

34.1 Status

Use this menu to look at packet statistics, interface status, and basic device information. See [Chapter 5 on page 85](#) for background information. To open this menu, enter 1 in menu 24.

Figure 199 Menu 24.1: System Maintenance - Status

```

Menu 24.1 - System Maintenance - Status                               10:57:51
                                                                    Wed. Jun. 07, 2006

Port  Status      TxPkts    RxPkts    Cols    Tx B/s    Rx B/s    Up Time
WAN   Down         124        0         0        0         0         0:00:00
LAN   100M/Full    9290      8691      0        272      128      1:48:14
WLAN  Down         402        332      0         0         0         0:00:07
Port  Ethernet Address      IP Address      IP Mask      DHCP
WAN   00:A0:C5:57:40:5B  43      0.0.5.0      0.074.0      None
LAN   00:A0:C5:57:40:5A      192.168.1.1    255.255.255.0  Server
WLAN  00:A0:C5:57:40:5A

System up Time:      1:24:52

Name: P870HW-I1.Zyxel.com
Routing: IP
ZyNOS F/W Version: V3.50 (RM.0)b8 | 06/09/2006

Press Command:

COMMANDS: 1-Drop WAN 9-Reset Counters  ESC-Exit

```

The following table describes the labels in this menu.

Table 146 Menu 24.1: System Maintenance - Status

FIELD	DESCRIPTION
Current Time	This field displays your ZyXEL Device's present time.
Current Date	This field displays your ZyXEL Device's present date.
Port	This field displays the ZyXEL Device's ports.

Table 146 Menu 24.1: System Maintenance - Status (continued)

FIELD	DESCRIPTION
Status	For the WAN port, this field depends on the encapsulation. For Ethernet encapsulation: Down - line is down Up - line is up or connected For PPP over Ethernet (PPPoE) encapsulation: Down - line is down Up - line is up or connected Idle - line (ppp) idle Dial - starting to trigger a call Drop - dropping a call For the LAN port, this field displays one of the following values: Down - there are no LAN connections Up - line is at least one LAN connection For the WLAN port, this field displays one of the following values: Down - the wireless interface is disabled Up - the wireless interface is enabled
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Cols	This is the number of collisions 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 amount of time this port has been up.
Port	This field displays the ZyXEL Device's ports.
Ethernet Address	This field displays the MAC address of this port.
IP Address	This field displays the IP address currently assigned to this port.
IP Mask	This field displays the subnet mask currently assigned to this port.
DHCP	This field displays the DHCP role the ZyXEL Device plays on this port.
System up Time	This is the total time the ZyXEL Device has been on.
Name	This is the system name and domain name, used for identification purposes.
Routing	This field displays the type of routing the ZyXEL Device uses.
ZyNOS F/W Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Press Command	Enter the number of the command you would like to perform, and press [ENTER]. You might not see the number appear, but the command will work.

34.2 Information

Use this menu to look at basic device information and LAN interface settings. See [Chapter 5 on page 85](#) for background information. To open this menu, enter 1 in menu 24.2.

Figure 200 Menu 24.2.1: System Maintenance - Information

```

Menu 24.2.1 - System Maintenance - Information

Name: P870HW-I1.Zyxel.com
Routing: IP
ZyNOS F/W Version: V3.50(RM.0)b8 | 06/09/2006
Country Code: 255

LAN
Ethernet Address: 00:A0:C5:57:40:5A
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

```

The following table describes the labels in this menu.

Table 147 Menu 24.2.1: System Maintenance - Information

FIELD	DESCRIPTION
Name	This is the system name and domain name, used for identification purposes.
Routing	This field displays the type of routing the ZyXEL Device uses.
ZyNOS F/W Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Country Code	This field displays the code for the place in which the ZyXEL Device is currently located. 255 is the default code.
LAN	
Ethernet Address	This field displays the MAC address of this port.
IP Address	This field displays the IP address currently assigned to this port.
IP Mask	This field displays the subnet mask currently assigned to this port.
DHCP	This field displays the DHCP role the ZyXEL Device plays on this port.

34.3 Change Console Port Speed

Note: The console port is internal and reserved for technician use only.

Use this menu to change the console port speed. To open this menu, enter 2 in menu 24.2.

Figure 201 Menu 24.2.2: System Maintenance - Change Console Port Speed

```

Menu 24.2.2 - System Maintenance - Change Console Port Speed

Console Port Speed: 9600

```

The following table describes the labels in this menu.

Table 148 Menu 24.2.2: System Maintenance - Change Console Port Speed

FIELD	DESCRIPTION
Console Port Speed	Select the console port speed.

34.4 Syslog Logging

Use this menu to configure the ZyXEL Device to send log messages to a syslog server. See [Chapter 19 on page 237](#) for background information. To open this menu, enter 2 in menu 24.3.

Figure 202 Menu 24.3.2: System Maintenance - Syslog Logging

```

Menu 24.3.2 - System Maintenance - Syslog Logging

Syslog:
Active= No
Syslog Server IP Address= 0.0.0.0
Log Facility= Local 1

```

The following table describes the labels in this menu.

Table 149 Menu 24.3.2: System Maintenance - Syslog Logging

FIELD	DESCRIPTION
Syslog	The ZyXEL Device can send logs 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 the file the syslog server uses for the ZyXEL Device. 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.

34.5 Call-Triggering Packet

Use this menu to look at information about the packet that triggered a dial-out call. The packet is displayed in an easy-to-read format. To open this menu, enter 4 in menu 24.3.

Figure 203 Menu 24.3.4: Call-Triggering Packet (Example)

```

IP Frame: ENET0-RCV Size: 44/ 44   Time: 17:02:44.262
Frame Type:
  IP Header:
    IP Version           = 4
    Header Length        = 20
    Type of Service      = 0x00 (0)
    Total Length         = 0x002C (44)
    Identification       = 0x0002 (2)
    Flags                 = 0x00
    Fragment Offset      = 0x00
    Time to Live          = 0xFE (254)
    Protocol              = 0x06 (TCP)
    Header Checksum       = 0xFB20 (64288)
    Source IP             = 0xC0A80101 (192.168.1.1)
    Destination IP       = 0x00000000 (0.0.0.0)
  TCP Header:
    Source Port           = 0x0401 (1025)
    Destination Port      = 0x000D (13)
    Sequence Number       = 0x05B8D000 (95997952)
    Ack Number            = 0x00000000 (0)
    Header Length         = 24
    Flags                  = 0x02 (...S.)
    Window Size           = 0x2000 (8192)
    Checksum               = 0xE06A (57450)
    Urgent Ptr             = 0x0000 (0)
    Options                =
      0000: 02 04 02 00
  RAW DATA:
    0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E.....
    0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00  .....
    0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...

```

34.6 Diagnostic

Use this menu to check the ZyXEL Device's connections to other devices. To open this menu, enter 4 in menu 24.

Figure 204 Menu 24.4: System Maintenance - Diagnostic

```

Menu 24.4 - System Maintenance - Diagnostic

TCP/IP
  1. Ping Host
  2. WAN DHCP Release
  3. WAN DHCP Renewal
  4. PPPoE Setup Test

System
  11. Reboot System

Enter Menu Selection Number:

Host IP Address= N/A

```

The following table describes the labels in this menu.

Table 150 Menu 24.4: System Maintenance - Diagnostics

FIELD	DESCRIPTION
Ping Host	Select this if you want to ping a specific computer. Enter 1 in the Enter Menu Selection Number field, and then enter the IP address in the Host IP Address field.
WAN DHCP Release	Select this if you want to release the IP address, subnet mask, and other network information provided by the DHCP server.
WAN DHCP Renewal	Select this if you want to get a new IP address, subnet mask, and other network information from the DHCP server.
PPPoE Setup Test	Select this if you want to test the current PPPoE settings. You cannot run this test if you selected Ethernet in the Encapsulation field.
Reboot System	Use this screen to reboot the ZyXEL Device without turning the power off. This does not affect the ZyXEL Device's configuration.
Enter Menu Selection Number	Enter the test you want to perform.
Host IP Address	If you select Ping Host , enter the IP address of the computer you want the ZyXEL Device to ping.

CHAPTER 35

System Maintenance 24.5 - 24.7

This chapter covers menus 24.5 through 24.7. Use these menus to backup and restore your configuration file, as well as upload new firmware and configuration files.

35.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password and 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. 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) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version.

Table 151 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	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.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the ZyXEL Device.

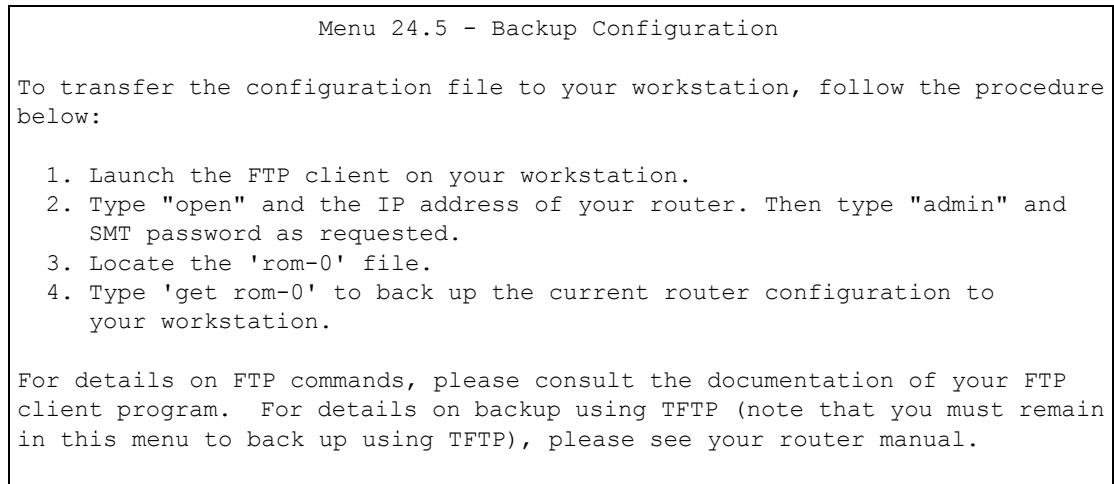
35.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current ZyXEL Device configuration to your computer. Backup is highly recommended once your ZyXEL Device is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms “download” and “upload” are relative to the computer. Download means to transfer from the ZyXEL Device to the computer, while upload means from your computer to the ZyXEL Device.

35.2.1 Backup Configuration Using FTP

Enter 5 in **Menu 24 – System Maintenance** to get the following screen.

Figure 205 Menu 24.5: Backup Configuration

35.2.2 Using the FTP command from the DOS Prompt

- 1 Launch the FTP client on your computer.
- 2 Enter "open" 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.

Figure 206 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: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

The following table describes some of the commands that you may see in third party FTP clients.

Table 152 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user ID 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).

35.2.3 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 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

- 3 Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
- 5 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 and the SMT 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 ZyXEL Device to the computer and “binary” to set binary transfer mode.

35.2.4 Example: TFTP Command

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.

The following table describes some of the fields that you may see in third party TFTP clients.

Table 153 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.2 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.

35.2.5 Backup Via Console Port

Note: The console port is internal and reserved for technician use only.

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

- 1 Display menu 24.5 and enter “y” at the following screen.

Figure 207 System Maintenance: Backup Configuration

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

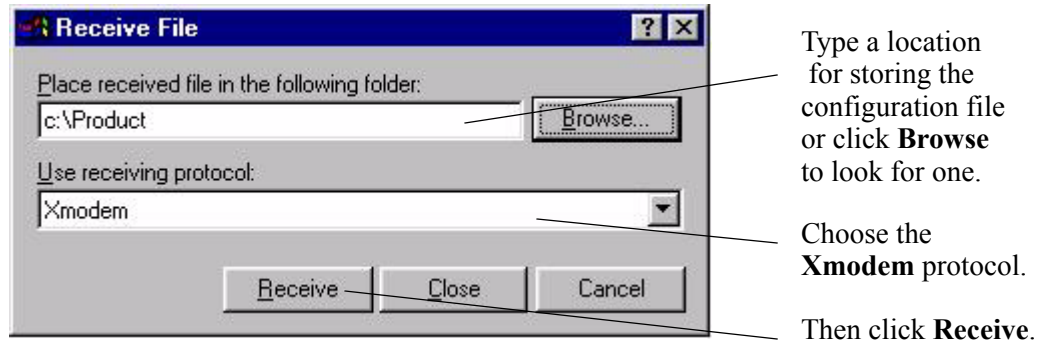
- 2 The following screen indicates that the Xmodem download has started.

Figure 208 System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any time.
Starting XMODEM download...
```

- 3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 209 Backup Configuration Example



- 4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 210 Successful Backup Confirmation Screen

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

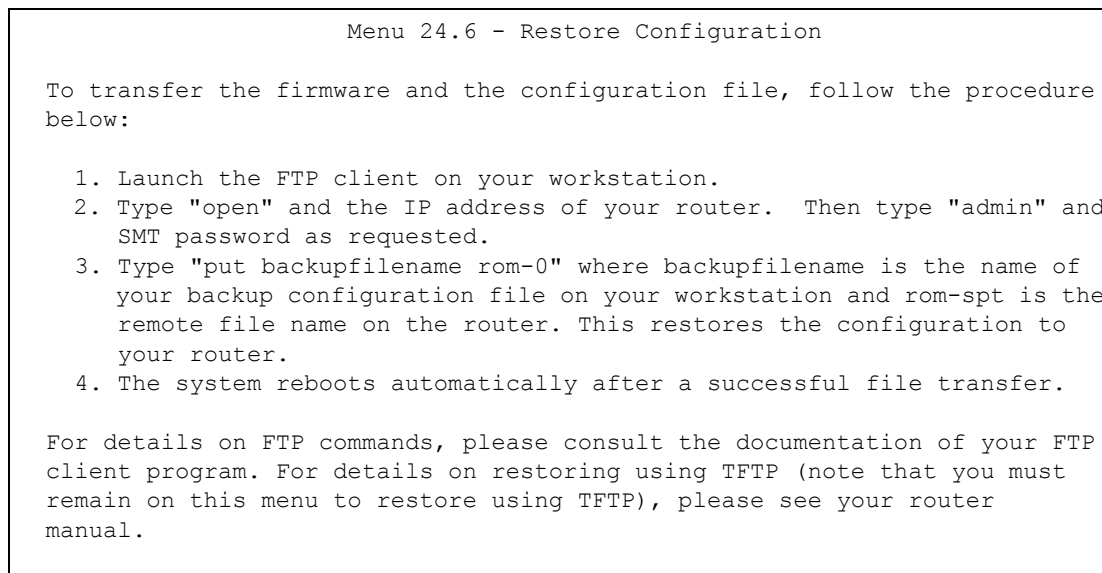
35.3 Restore Configuration

Menu 24.6 — System Maintenance – Restore Configuration allows you to restore the configuration via FTP or TFTP to your ZyXEL Device. The preferred method is FTP. Note that this function erases the current configuration before restoring the previous backup configuration; please do not attempt to restore unless you have a backup configuration stored on disk. To restore configuration using FTP or TFTP is the same as uploading the configuration file, please refer to the following sections on FTP and TFTP file transfer for more details. The ZyXEL Device restarts automatically after the file transfer is complete.

35.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Figure 211 Menu 24.6: Restore Configuration

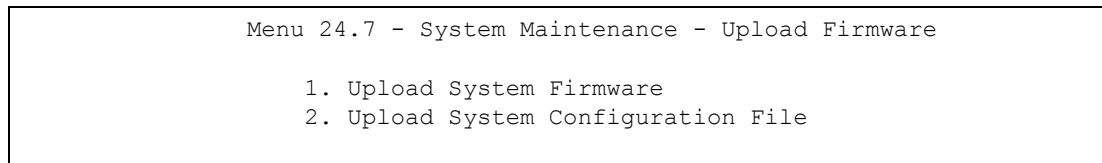


35.4 Uploading Firmware and Configuration Files

Menu 24.7 – System Maintenance – Upload Firmware allows you to upgrade the firmware and the configuration file.

Note: WARNING! PLEASE WAIT A FEW MINUTES FOR THE ZyXEL Device TO RESTART AFTER FIRMWARE OR CONFIGURATION FILE UPLOAD. INTERRUPTING THE UPLOAD PROCESS MAY PERMANENTLY DAMAGE YOUR ZyXEL Device.

Figure 212 Menu 24.7: System Maintenance - Upload Firmware



The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

35.4.1 Firmware Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyXEL Device, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 213 Menu 24.7.1: System Maintenance - Upload System Firmware

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

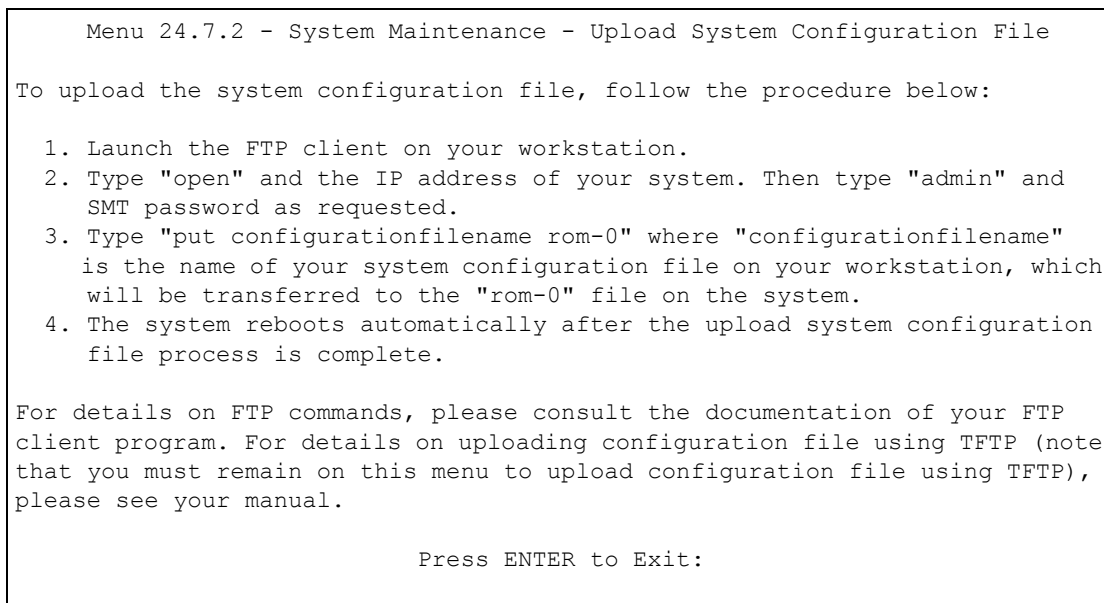
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "admin" and
   SMT password as requested.
3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
   of your firmware upgrade file on your workstation and "ras" is the
   remote file name on the system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

35.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 214 Menu 24.7.2: System Maintenance - Upload System Configuration File

To transfer the firmware and the configuration file, follow these examples:

35.4.3 Using the FTP command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter "open" 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 "put" to transfer files from the computer to the ZyXEL Device, e.g., put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the ZyXEL Device and renames it "ras". Similarly "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the ZyXEL Device and renames it "rom-0". Likewise "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.

Figure 215 FTP Session Example

```
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: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands that you may find in third party FTP clients are listed earlier in this chapter.

35.4.4 TFTP File Upload

The ZyXEL Device also 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 transfer the firmware and 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 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter the command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
- 5 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the firmware is “ras” and the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT 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 ZyXEL Device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

35.4.5 Example: TFTP Command

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 ZyXEL 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 ZyXEL Device).

Commands that you may see in third party TFTP clients are listed earlier in this chapter.

35.4.6 Uploading Via Console Port

Note: The console port is internal and reserved for technician use only.

FTP or TFTP are the preferred methods for uploading firmware to your ZyXEL Device. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyXEL Device via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

35.4.7 Uploading Firmware File Via Console Port

Note: The console port is internal and reserved for technician use only.

Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 – System Maintenance – Upload System Firmware**, then follow the instructions as shown in the following screen.

Figure 216 Menu 24.7.1 as seen using the Console Port

```

Menu 24.7.1 - System Maintenance - Upload System Firmware
To upload system firmware:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   router.
Warning: Proceeding with the upload will erase the current system
firmware.
Do You Wish To Proceed:(Y/N)

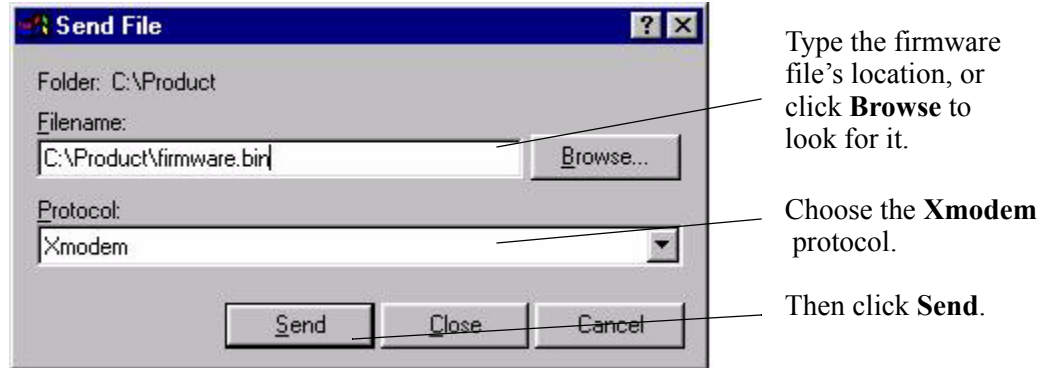
```

After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

35.4.8 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 217 Example Xmodem Upload



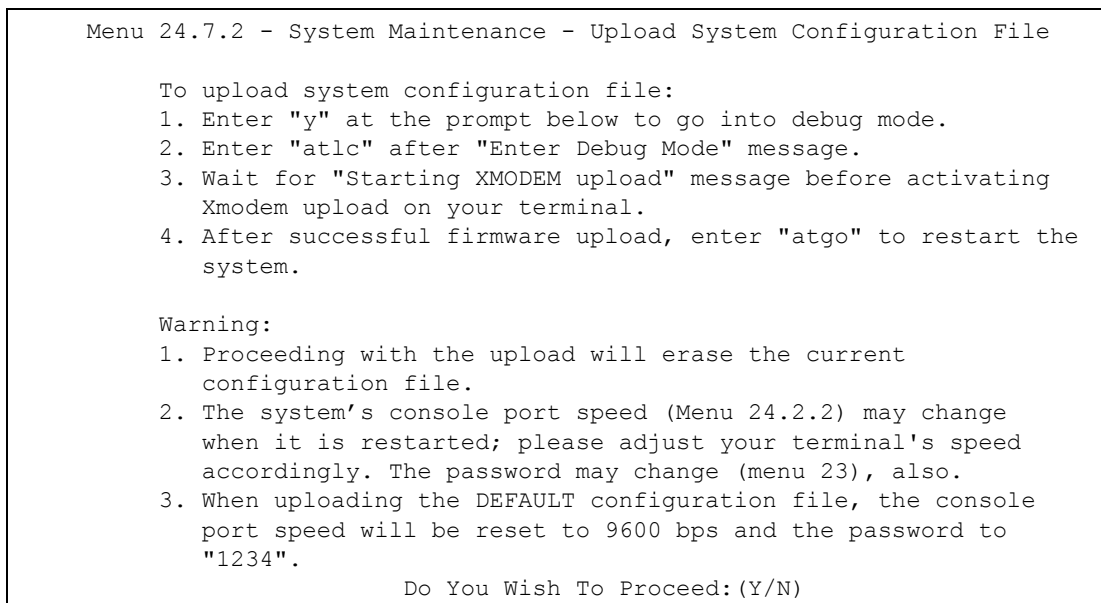
After the firmware upload process has completed, the ZyXEL Device will automatically restart.

35.4.9 Uploading Configuration File Via Console Port

Note: The console port is internal and reserved for technician use only.

- 1 Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 – System Maintenance – Upload System Configuration File**. Follow the instructions as shown in the next screen.

Figure 218 Menu 24.7.2 as seen using the Console Port

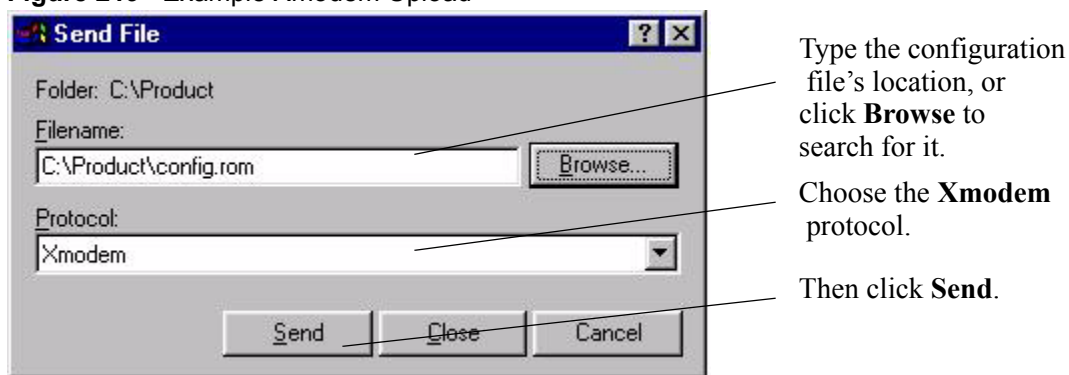


- 2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.
- 3 Enter "atgo" to restart the ZyXEL Device.

35.4.10 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 219 Example Xmodem Upload



After the configuration upload process has completed, restart the ZyXEL Device by entering "atgo"

CHAPTER 36

System Maintenance 24.8 - 24.11

This chapter covers menus 24.8 through 24.11. Use these menus to get a use CI commands, see how long you have accessed the Internet and how much budgeted time remains, set the current date and time, and configure remote access to the ZyXEL Device.

36.1 Command Interpreter Mode

Use this menu to use CI commands. To do so, enter 8 in menu 24.

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. A list of valid commands can be found by entering `help` or `?`.

Figure 220 Valid CI Commands

```
P870HW-I1> ?
Valid commands are:
sys                exit                device                ether
poe                config                vdsl                 wlan
ip                 ppp                 bridge                bm
certificates       8021x                autoSec              radius
```

Type `exit` to return to the SMT main menu.

36.2 Budget Management

This menu is only applicable your Internet connection uses PPPoE encapsulation. Use this menu to look at how long you have accessed the Internet and how much budgeted time remains. See [Chapter 26 on page 269](#) for related settings. To open this menu, enter 1 in menu 24.9.

Figure 221 Menu 24.9.1: Budget Management

Menu 24.9.1 - Budget Management		
Remote Node	Connection Time/Total Budget	Elapsed Time/Total Period
1.ChangeMe	No Budget	No Budget
Reset Node (0 to update screen):		

The following table describes the labels in this menu.

Table 154 Menu 24.9.1: Budget Management

FIELD	DESCRIPTION
Remote Node	This field displays the name of the ISP.
Connection Time/ Total Budget	This field displays the number of minutes calls have lasted and the maximum number of minutes calls can last. If there is no maximum number, this field displays No Budget .
Elapsed Time/Total Period	This field displays the how much time has passed since the allocated budget reset and how much time must pass altogether before the allocated budget resets.
Reset Node	Enter the number of the ISP whose connection time you want to reset immediately, or enter 0 to update the screen.

36.3 Call History

This menu is only applicable your Internet connection uses PPPoE encapsulation. Use this menu to look at previous calls made to establish the Internet connection. See [Chapter 26 on page 269](#) for related settings. To open this menu, enter 2 in menu 24.9.

Figure 222 Menu 24.9.2: Call History

Menu 24.9.2 - Call History							
	Phone Number	Dir	Rate	#call	Max	Min	Total
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
Enter Entry to Delete(0 to exit):							

The following table describes the labels in this menu.

Table 155 Menu 24.9.2: Call History

FIELD	DESCRIPTION
Phone Number	This field displays the PPPoE service name.
Dir	This field displays whether the call was incoming or outgoing.
Rate	This field displays the transfer rate of the call.
#call	This field displays the number of calls made to or received from that telephone number.
Max	This field displays the length of time of the longest telephone call.
Min	This field displays the length of time of the shortest telephone call.
Total	This field displays the total length of time of all the telephone calls to/from that telephone number.
Enter Entry to Delete	Enter the number of an entry to delete, or enter 0 to return to the previous menu.

36.4 Time and Date Setting

Use this menu to change your ZyXEL Device's time and date. See [Chapter 18 on page 229](#) for background information. To open this menu, enter 10 in menu 24.

Figure 223 Menu 24.10: Time and Date Setting

```

Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= Manual
Time Server Address= N/A

Current Time:                11 : 02 : 11
New Time (hh:mm:ss):        11  01  32

Current Date:                2006 - 06 - 07
New Date (yyyy-mm-dd):      2006  06  07

Time Zone= (GMT+03:00) Baghdad, Kuwait, Nairobi, Riyadh, Moscow

Daylight Saving= No
Start Date (mm-nth-week-hr): Jan. - 1st - Sun.(01) - 00
End Date (mm-nth-week-hr):   Jan. - 1st - Sun.(01) - 00

```

The following table describes the labels in this menu.

Table 156 Menu 24.10: Time and Date Setting

FIELD	DESCRIPTION
Time Protocol	<p>You can update the current date and time manually, or the ZyXEL Device can synchronize with a time server.</p> <p>Manual means you update the current date and time manually.</p> <p>If the ZyXEL Device synchronizes with a time server, select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>The default, NTP (RFC 1305), is similar to Time (RFC 868).</p>
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.
Current Time	This field displays the current time in the ZyXEL Device.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the time you opened this menu. Enter the new time in this field.
Current Date	This field displays the current date in the ZyXEL Device.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the time you opened this menu. Enter the new date in this field.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	<p>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.</p> <p>Select this option if you use Daylight Saving Time.</p>

Table 156 Menu 24.10: Time and Date Setting (continued)

FIELD	DESCRIPTION
Start Date	<p>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:</p> <p>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 April, 1st, Sun., 2.</p> <p>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 March, Last, Sunday. The time you type in the last field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Enable Daylight Saving. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select October, Last, Sunday, 2.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select October, Last, Sunday. The time you type in the last field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>

36.5 Remote Management Control

Use this screen to configure through which interface(s) and from which IP address(es) users can use various protocols to manage the ZyXEL Device. See [Chapter 16 on page 205](#) for background information. To open this menu, enter 11 in menu 24.

Figure 224 Menu 24.11: Remote Management Control

Menu 24.11 - Remote Management Control		
TELNET Server:	Port = 23	Access = ALL
	Secure Client IP = 0.0.0.0	
FTP Server:	Port = 21	Access = ALL
	Secure Client IP = 0.0.0.0	
SSH Server:	Certificate = newDefault	
	Port = 22	Access = ALL
	Secure Client IP = 0.0.0.0	
HTTPS Server:	Certificate = newDefault	
	Authenticate Client Certificates = No	
	Port = 443	Access = ALL
	Secure Client IP = 0.0.0.0	
HTTP Server:	Port = 80	Access = ALL
	Secure Client IP = 0.0.0.0	
SNMP Service:	Port = 161	Access = ALL
	Secure Client IP = 0.0.0.0	
DNS Service:	Port = 53	Access = ALL
	Secure Client IP = 0.0.0.0	

The following table describes the labels in this menu.

Table 157 Menu 24.11: Remote Management Control

FIELD	DESCRIPTION
	These fields are similar for all servers and services.
Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secure Client IP	Enter an IP address to only allow the computer with this IP address to access the ZyXEL Device using this service. Enter 0.0.0.0 to allow any computer to access the ZyXEL Device using this service.
	These fields are used by specific servers and services.
SSH Server	
Certificate	Select the certificate the ZyXEL Device provides to clients using this service.
HTTPS Server	
Certificate	Select the certificate the ZyXEL Device provides to clients using this service.
Authenticate Client Certificates	This field is disabled if you have not set up any trusted certification authorities. Select this if you want the trusted certification authorities to check the clients' certificates before the ZyXEL Device allows access using this service.

CHAPTER 37

IP Routing Policy Setup

Use this menu to look at and configure policy routes.

37.1 Policy Route

Traditionally, routing is based on the destination address only and the ZyXEL Device 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. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

37.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – Organizations can allocate bandwidth to traffic that matches the routing policy and prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The ZyXEL Device performs NAT by default for traffic going to or from the **ge1** interface. Routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

37.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

The actions that can be taken include:

- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

37.4 IP Routing Policy Summary

Use this menu to look at policy routes. To open this menu, enter 25 in the main menu.

Figure 225 Menu 25: IP Routing Policy Summary

#		A	Criteria/Action
001	N	SA=1.1.1.1-1.1.1.1 DA=2.2.2.2-2.2.2.5 SP=20-25 DP=20-25 P=6 T=NM PR=0	GW=192.168.1.1 T=MT PR=0
002	N		
003	N		
004	N		
005	N		
006	N		
		Select Command= None	Select Rule= N/A

The following table describes the labels in this menu.

Table 158 Menu 25: IP Routing Policy Summary

FIELD	DESCRIPTION
#	This field displays the rule number.
Criteria/Action	See Table 159 on page 340 .
Select Command Select Rule	In the Select Command field, press the [SPACEBAR] to select what change you would like to make. For some actions, enter the rule number in the Select Rule field to specify on which rule you would like to apply the action.

Table 159 Menu 25: IP Routing Policy Summary, Abbreviations

ABBREVIATION	MEANING
SA	Source IP Address
SP	Source Port
DA	Destination IP Address
DP	Destination Port
P	IP layer 4 protocol number (TCP=6, UDP=17...)
T	Type of service of incoming packet

Table 159 Menu 25: IP Routing Policy Summary, Abbreviations (continued)

ABBREVIATION	MEANING
PR	Precedence of incoming packet
Action GW	Gateway IP address
T	Outgoing Type of service
P	Outgoing Precedence
Service NM	Normal
MD	Minimum Delay
MT	Maximum Throughput
MR	Maximum Reliability
MC	Minimum Cost

37.5 IP Routing Policy Setup

Use this menu to configure policy routes. To open this menu, select **Edit** and enter the appropriate rule number in menu 25.

Figure 226 Menu 25.1: IP Routing Policy Setup

```

Menu 25.1 - IP Routing Policy Setup

Rule Index= 1                               Active= No
Criteria:
  IP Protocol      = 0
  Type of Service= Don't Care                Packet length= 0
  Precedence      = Don't Care                Len Comp= N/A
Source:
  addr start= 0.0.0.0                       end= N/A
  port start= N/A                           end= N/A
Destination:
  addr start= 0.0.0.0                       end= N/A
  port start= N/A                           end= N/A
Action= Matched
  Gateway addr= 0.0.0.0                     Log= No
  Type of Service= Don't Care
  Precedence      = Don't Care
Edit policy to packets received from= No
    
```

The following table describes the labels in this menu.

Table 160 Menu 25.1: IP Routing Policy Setup

FIELD	DESCRIPTION
Rule Index	This is the index number of the routing policy selected in Menu 25 - IP Routing Policy Summary .
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate the policy.

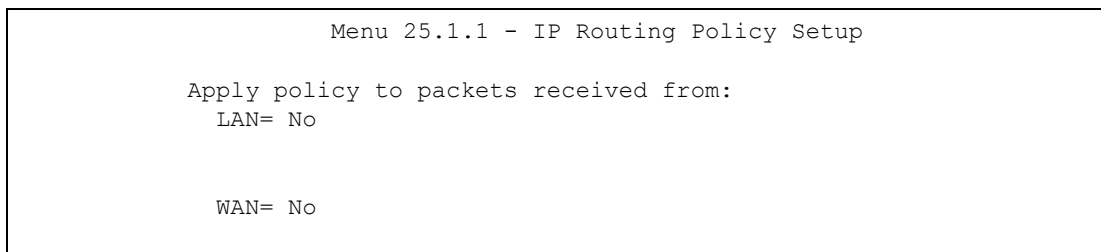
Table 160 Menu 25.1: IP Routing Policy Setup (continued)

FIELD	DESCRIPTION
Criteria	
IP Protocol	Enter a number that represents an IP layer 4 protocol, for example, UDP=17, TCP=6, ICMP=1 and Don't care=0.
Type of Service	Prioritize incoming network traffic by choosing from Don't Care, Normal, Min Delay, Max Thruput or Max Reliable .
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from 0 to 7 or Don't Care .
Packet Length	Type the length of incoming packets (in bytes). The operators in the Len Comp (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from Equal, Not Equal, Less, Greater, Less or Equal or Greater or Equal .
Source	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria Matched or Not Matched.
Gateway addr	Enter the IP address of the gateway to which the ZyXEL Device forwards the packet. The gateway is an immediate neighbor of your ZyXEL Device and must be on the same subnet as the ZyXEL Device, if it is on the LAN, or the IP address of a remote node, if it is on the WAN. Enter 0.0.0.0 to specify the default gateway.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing Don't Care, Normal, Min Delay, Max Thruput, Max Reliable or Min Cost .
Precedence	Set the new outgoing packet precedence value. Values are 0 to 7 or Don't Care .
Log	Press [SPACE BAR] and then [ENTER] to select Yes to make an entry in the system log when a policy is executed.
Edit policy to packets received from	If you want to specify the ports from which traffic comes to which the policy applies, press [SPACE BAR] to select Yes and press [ENTER]. Menu 25.1.1 appears.

37.6 IP Routing Policy Setup

Use this menu to specify the ports from which traffic comes to which the policy routes apply. To open this menu, select **Yes** in **Edit policy to packets received from** in menu 25.1.

Figure 227 Menu 25.1.1: IP Routing Policy Setup



The following table describes the labels in this menu.

Table 161 Menu 25.1.1: IP Routing Policy Setup

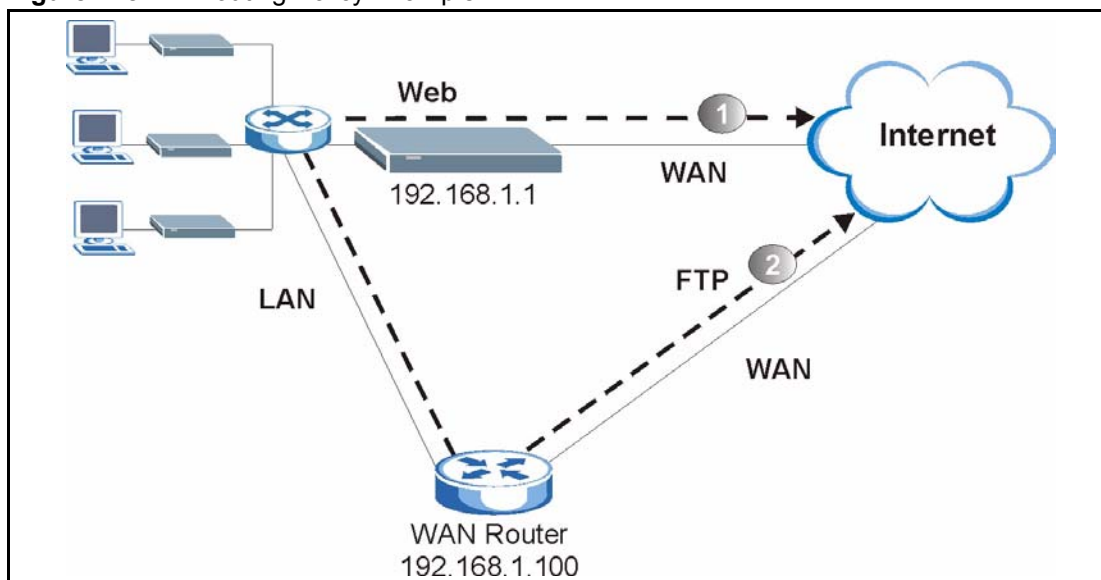
FIELD	DESCRIPTION
LAN	Select this if you want to apply the policy to packets received on this port.
WAN	Select this if you want to apply the policy to packets received on this port.

37.7 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.

Figure 228 IP Routing Policy Example



To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the ZyWALL, follow the steps as shown next.

1 Create a rule in **Menu 25.1 - IP Routing Policy Setup** as shown next.

Figure 229 IP Routing Policy Example 1

```
Menu 25.1 - IP Routing Policy Setup

Rule Index= 1                               Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care                 Packet length= 10
  Precedence      = Don't Care                 Len Comp= Equal
Source:
  addr start= 192.168.1.33                   end= 192.168.1.64
  port start= 0                               end= N/A
Destination:
  addr start= 0.0.0.0                         end= N/A
  port start= 80                               end= 80
Action= Matched
  Gateway Type= IP Address
  Gateway addr  = 192.168.1.1                 Redirect packet= N/A
  Type of Service= Max Thruput                Log= No
  Precedence    = 0
Edit policy to packets received from= No

                               Press ENTER to Confirm or ESC to Cancel:
```

- 2** Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.
- 3** Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.
- 4** Create another rule in menu 25.1 for this rule to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

Figure 230 IP Routing Policy Example 2

```

Menu 25.1 - IP Routing Policy Setup

Rule Index= 2                               Active= No
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care                Packet length= 10
  Precedence      = Don't Care                Len Comp= Equal
Source:
  addr start= 0.0.0.0                       end= N/A
  port start= 0                              end= N/A
Destination:
  addr start= 0.0.0.0                       end= N/A
  port start= 20                             end= 21
Action= Matched
  Gateway Type= IP Address
  Gateway addr  = 192.168.1.100             Redirect packet= N/A
  Type of Service= Don't Care             Log= No
  Precedence      = Don't Care
Edit policy to packets received from= No

                                Press ENTER to Confirm or ESC to Cancel:

```

- 5** Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.
- 6** Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

CHAPTER 38

Schedule Setup

Use this menu to look at and configure the schedule sets in the ZyXEL Device.

38.1 Schedule Set Overview

Call scheduling (applicable for PPPoE encapsulation only) allows the ZyXEL Device to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler that lets you specify a time period to record a television program in a VCR or TiVo.

38.2 Schedule Setup

This menu is only applicable if your Internet connection uses PPPoE encapsulation. Use this menu to look at the schedule sets in the ZyXEL Device. To open this menu, enter 26 in the main menu.

Figure 231 Menu 26: Schedule Setup

Menu 26 - Schedule Setup			
Schedule Set #	Name	Schedule Set #	Name
1	_____	7	_____
2	_____	8	_____
3	_____	9	_____
4	_____	10	_____
5	_____	11	_____
6	_____	12	_____
Enter Schedule Set Number to Configure= 0 Edit Name= N/A			

The following table describes the labels in this menu.

Table 162 Menu 26: Schedule Setup

FIELD	DESCRIPTION
1-12	This field shows the beginning of the name of each schedule set. Lower numbered sets take precedence over higher numbered sets. This avoids scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node, then set 1 takes precedence over set 2, 3 and 4.
Enter Schedule Set Number to Configure	If you want to configure a schedule set, enter the number of the static route in this field, enter the name in the Edit Name field, and press [ENTER]. Menu 26.1 appears. If you want to delete a schedule set, enter the number of the static route in this field, leave the name blank in the Edit Name field, and press [ENTER].
Edit Name	Enter the name of the schedule set you want to configure, or leave this field blank to delete the specified schedule set.

38.3 Schedule Set Setup

This menu is only applicable if your Internet connection uses PPPoE encapsulation. Use this menu to configure the schedule sets in the ZyXEL Device. To open this menu, enter the number of the schedule set in the **Enter Schedule Set Number to Configure** field, enter the name of the schedule set in the **Edit Name** field, and press [ENTER] in menu 26.

Figure 232 Menu 26.1: Schedule Set Setup

```

Menu 26.1 Schedule Set Setup

Active= Yes
How Often= Once
Start Date (yyyy-mm-dd)= N/A
Once:
  Date (yyyy-mm-dd)= 2000 - 01 - 01
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On
    
```

The following table describes the labels in this menu.

Table 163 Menu 26.1: Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select Yes or No . Choose Yes and press [ENTER] to activate the schedule set.
How Often	Enter the start date when you wish the set to take effect in year-month-date format. Valid dates are from the present to 2036-February-5.
Start Date	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select Once or Weekly . Both these options are mutually exclusive. If Once is selected, then all weekday settings are N/A . When Once is selected, the schedule rule deletes automatically after the scheduled time elapses.
Once	
Date	If you selected Once in the How Often field above, then enter the date the set should activate here in year-month-date format.
Weekdays	If you selected Weekly in the How Often field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select Yes , then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.

Table 163 Menu 26.1: Schedule Set Setup (continued)

FIELD	DESCRIPTION
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.
Action	<p>Forced On means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the Duration field.</p> <p>Forced Down means that the connection is blocked whether or not there is a demand call on the line.</p> <p>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.</p>

CHAPTER 39

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

39.1 Problems Starting Up the ZyXEL Device

The following table identifies some remedies if you have problems starting up the ZyXEL Device.

Table 164 Troubleshooting Starting Up Your ZyXEL Device

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

39.2 Problems with the LAN

The following table identifies some remedies if you have problems with the LAN connections.

Table 165 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN lights do not turn on.	<p>Check your Ethernet cable connections (see the <i>Quick Start Guide</i> for details). Check for faulty Ethernet cables.</p>
	<p>Make sure your computer's Ethernet card is working properly.</p>
I cannot access the ZyXEL Device from the LAN.	<p>Make sure that the IP address and the subnet mask of the ZyXEL Device and your computer(s) are on the same subnet. See the appendices for information how to do this.</p>

39.3 Problems with the WAN

The following table identifies some remedies if you have problems with the Internet connection.

Table 166 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The DSL light is off.	<p>Check the telephone wire and connections between the ZyXEL Device DSL port and the wall jack.</p> <p>Make sure that the telephone company has checked your phone line and set it up for DSL service.</p> <p>If the problem persists, contact your ISP.</p>
I cannot get a WAN IP address from the ISP.	<p>The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name. Make sure you have provided the correct user name and password (if required) in Network > WAN > Internet Connection. Try spoofing your computer's MAC address in Network > WAN > Internet Connection. Try using your computer's host name in Maintenance > System > General, though this requires you to change your computer's host name to avoid duplication.</p> <p>If the problem persists, contact your ISP.</p>
I cannot access the Internet.	<p>Make sure the ZyXEL Device is turned on and connected to the network.</p> <p>Verify your WAN settings. Refer to the chapter on WAN setup.</p> <p>Make sure you entered the correct user name and password.</p> <p>If the problem persists, contact your ISP.</p>
The Internet connection disconnects.	<p>If you use PPPoE encapsulation, check the idle time-out setting. See Network > WAN > Internet Connection.</p> <p>If the problem persists, contact your ISP.</p>

39.4 Problems Accessing the ZyXEL Device

The following table identifies some remedies if you have problems accessing the ZyXEL Device.

Table 167 Troubleshooting Accessing the ZyXEL Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	The default password is 1234 . If you have changed the password and have now forgotten it, you have to reset the ZyXEL Device. See the Introduction for details.
I cannot access the web configurator.	Make sure pop-up windows, JavaScripts and Java permissions are allowed. See the following section. Make sure that there is not a console session (for example, telnet) running. Use the ZyXEL Device's WAN IP address when configuring from the WAN. Make sure your WAN connection is good. Use the ZyXEL Device's LAN IP address when configuring from the LAN. Make sure your LAN connection is good. Check that you have enabled web service access. This is the default setting in Management > Remote MGMT > WWW . If you have configured a secured client IP address, your computer's IP address must match it. See the chapter on remote management for details. Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access. If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL.

39.4.1 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.

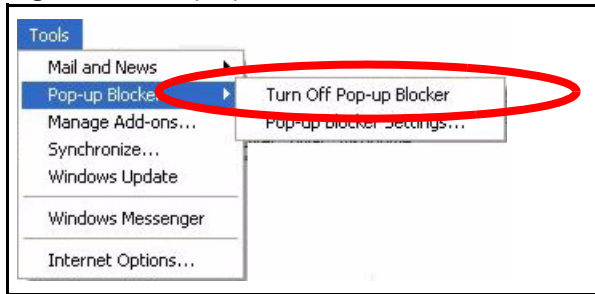
39.4.1.1 Internet Explorer Pop-up Blockers

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.

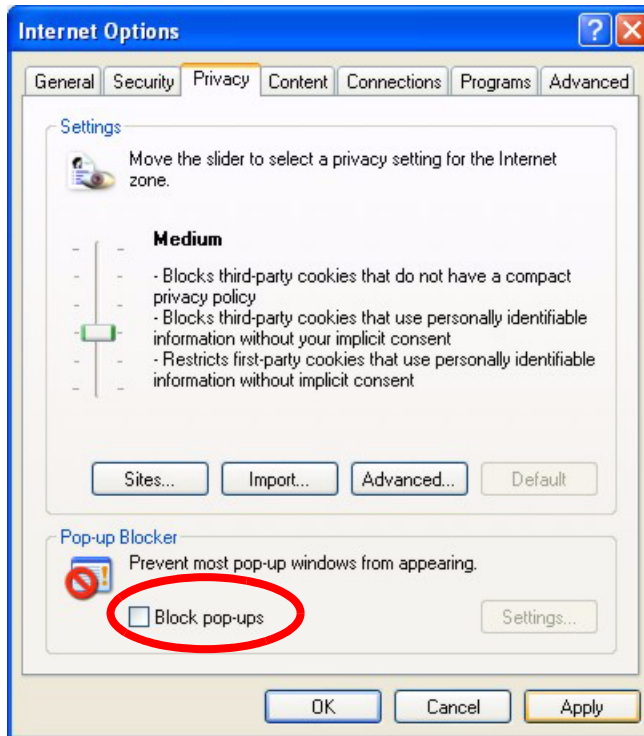
39.4.1.1.1 Disable pop-up Blockers

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

Figure 233 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.

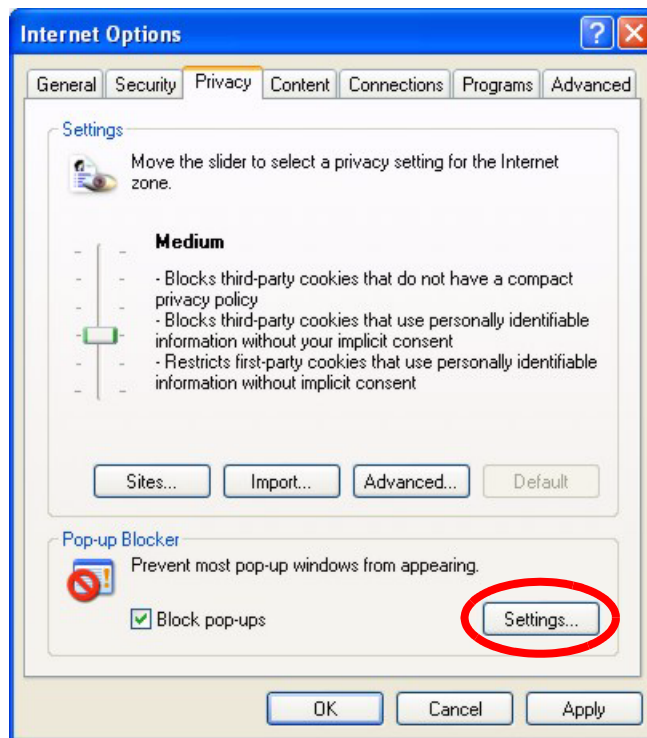
Figure 234 Internet Options

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

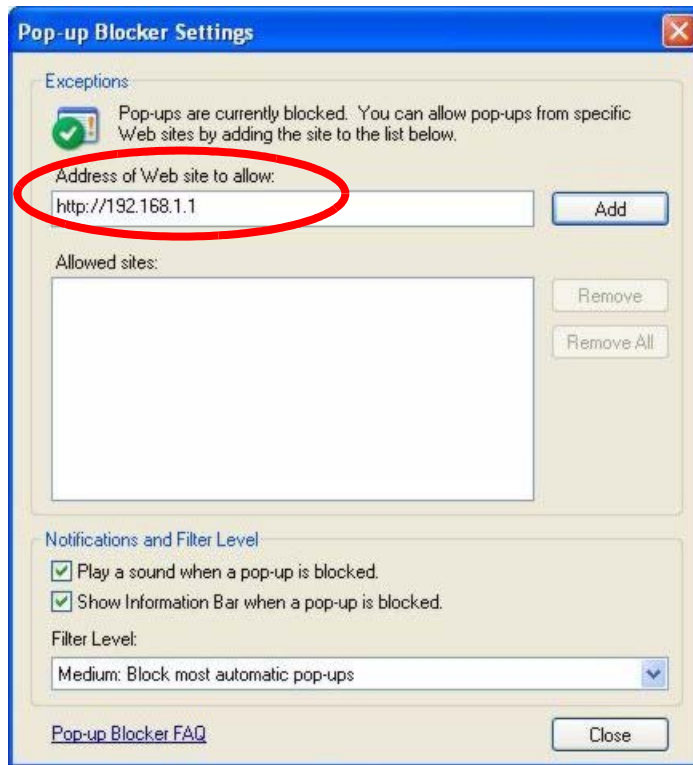
39.4.1.1.2 Enable pop-up Blockers with Exceptions

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 235 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 236 Pop-up Blocker Settings

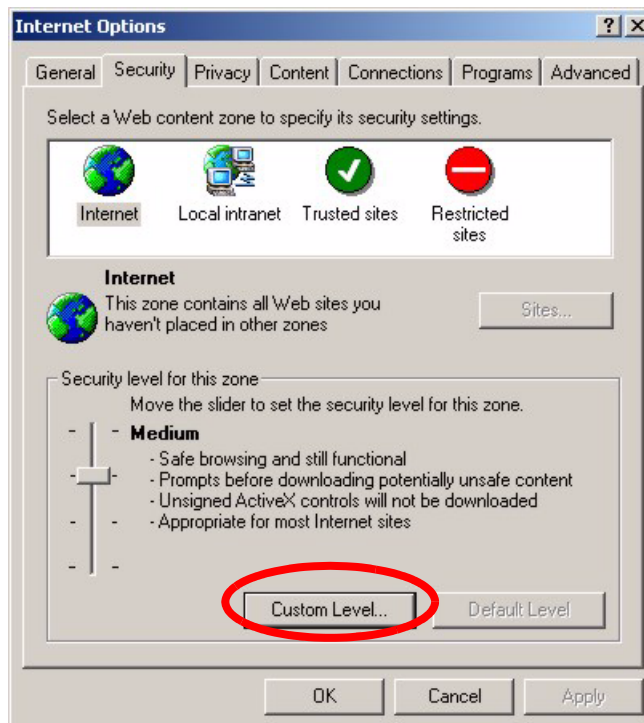
5 Click **Close** to return to the **Privacy** screen.

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

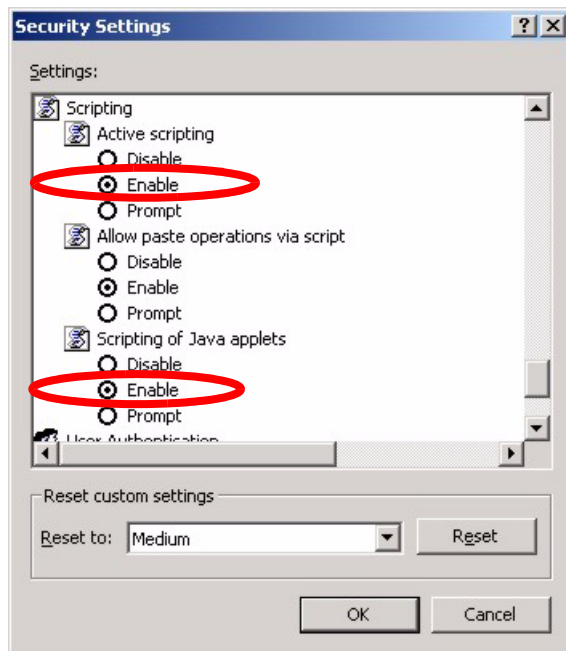
39.4.1.2 JavaScripts

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.

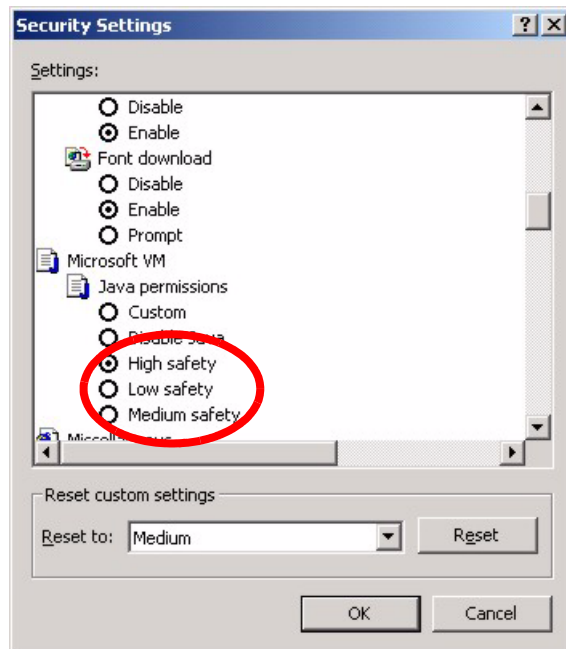
Figure 237 Internet Options

- 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 238 Security Settings - Java Scripting

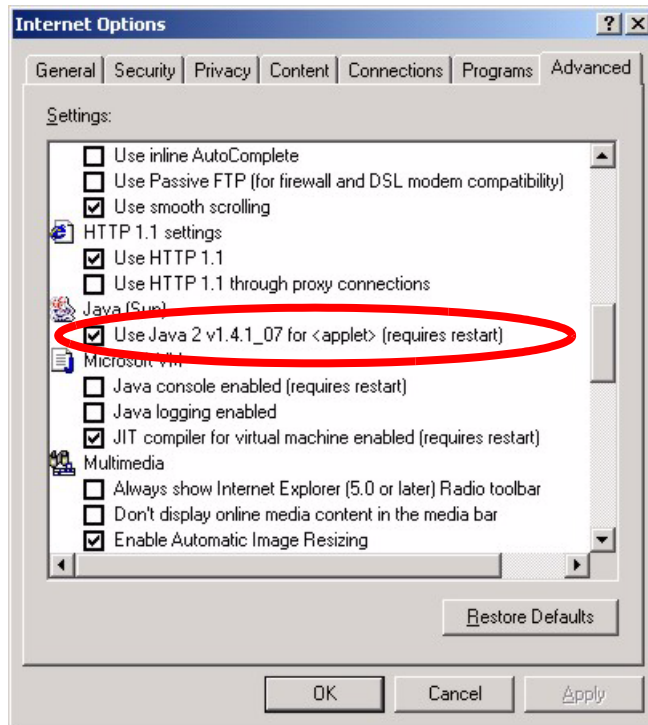
39.4.1.3 Java Permissions

- 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 239 Security Settings - Java

39.4.1.3.1 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.

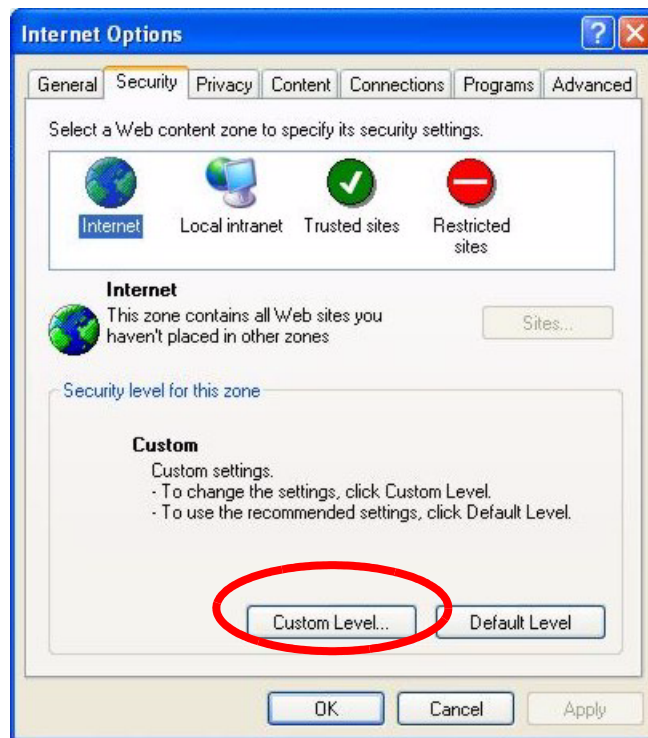
Figure 240 Java (Sun)

39.4.2 ActiveX Controls in Internet Explorer

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

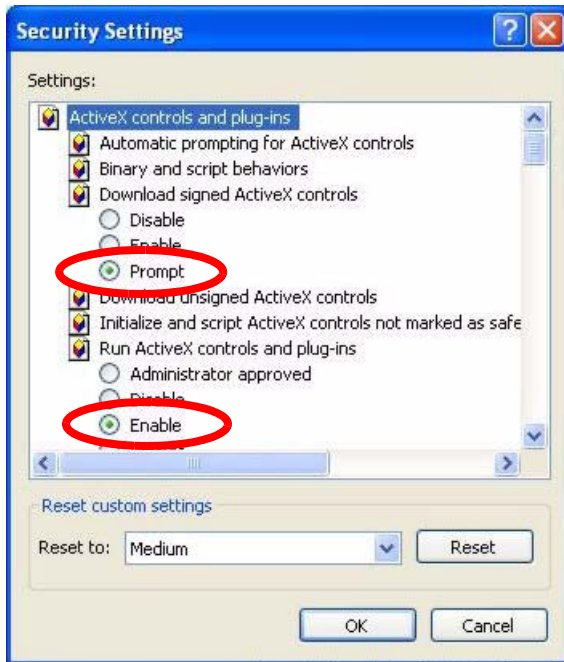
Screen shots for Internet Explorer 6 are shown. Steps may vary depending on your version of Internet Explorer.

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

Figure 241 Internet Options Security

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

Figure 242 Security Setting ActiveX Controls



Appendix A

Product Specifications

The values are accurate at the time of writing.

Table 168 Device Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Dimensions (W x D x H)	205 mm (L) x 160 mm (D) x 45 mm (H)
Power Specification	12 V AC 1.3 A
Built-in Switch	Four RJ-45 Ethernet ports, 10/100 Mbps, auto MDI/MDI-X
Antenna	2 dBi
Operating Temperature	0° C ~ 40° C
Operating Humidity	20% ~ 85% RH (non-condensing)

Appendix B

Setting up Your Computer's IP Address

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

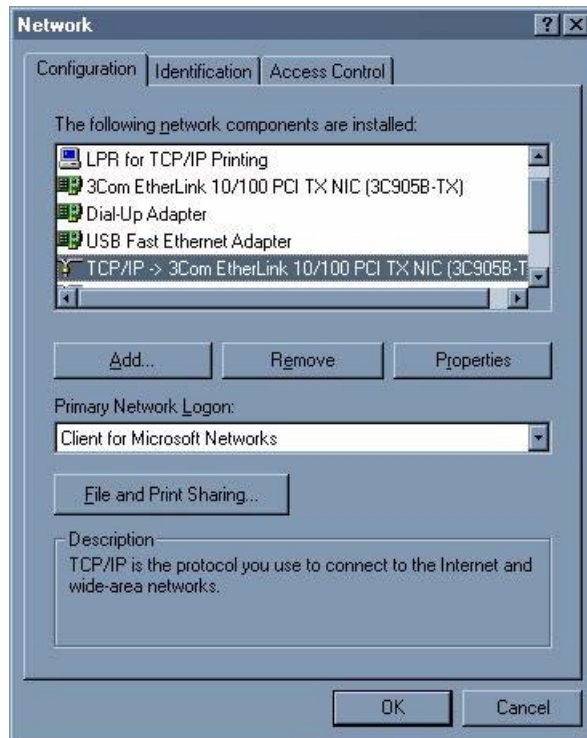
Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

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.

Windows 95/98/Me

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

Figure 243 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:

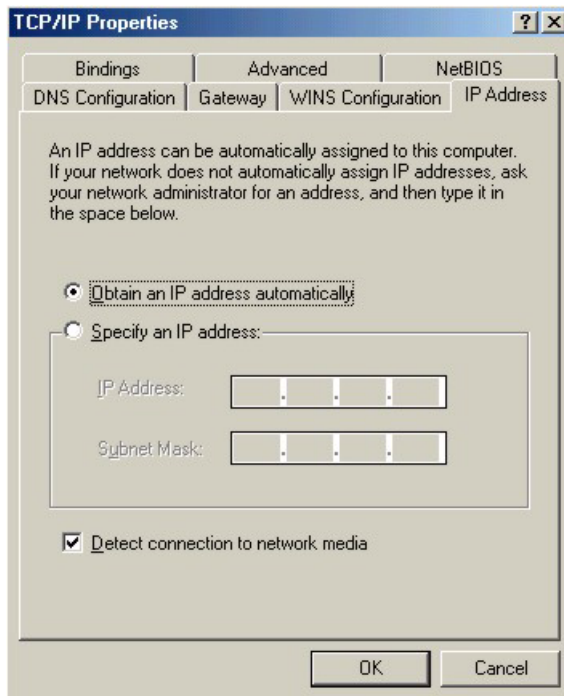
- 1** Click **Add**.
- 2** Select **Client** and then click **Add**.

- 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.

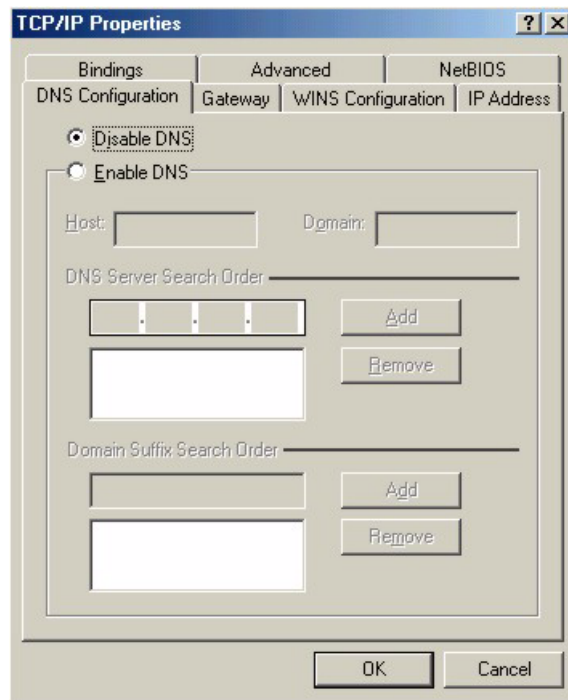
Configuring

- 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 244 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 245 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** Restart your computer when prompted.

Verifying Settings

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

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

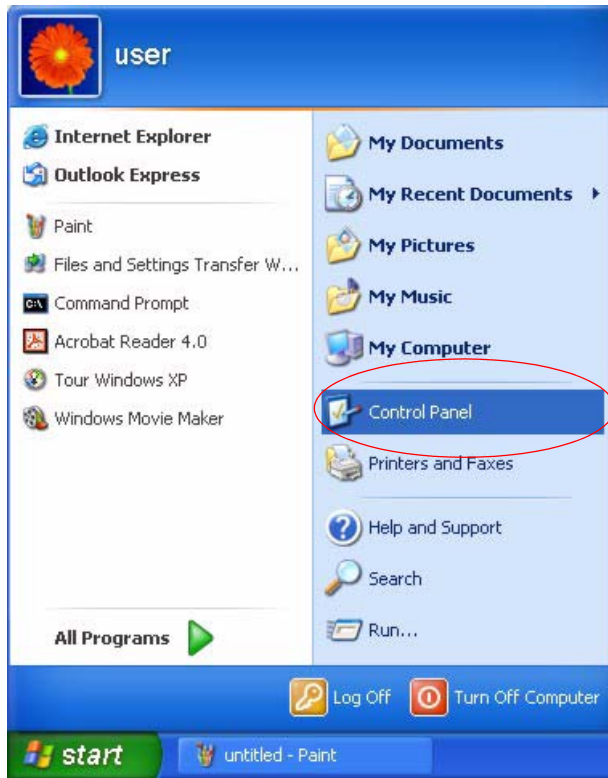
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

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

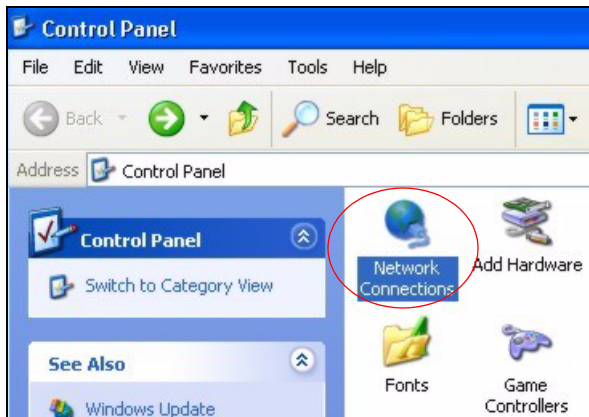
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 246 Windows XP: Start Menu

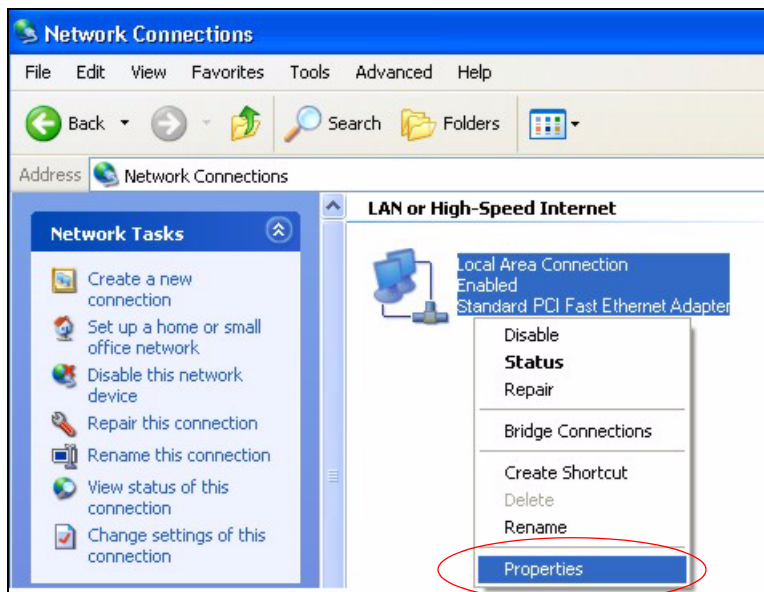


2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

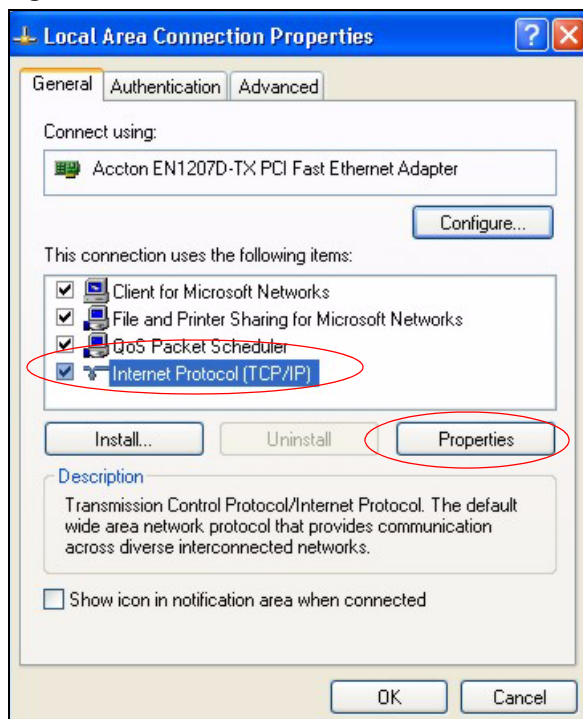
Figure 247 Windows XP: Control Panel



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

Figure 248 Windows XP: Control Panel: Network Connections: Properties

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

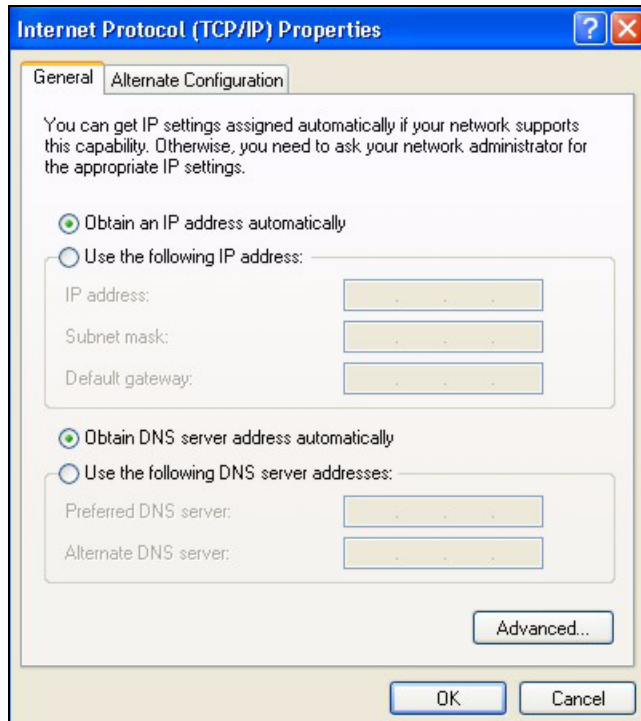
Figure 249 Windows XP: Local Area Connection Properties

- 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**.

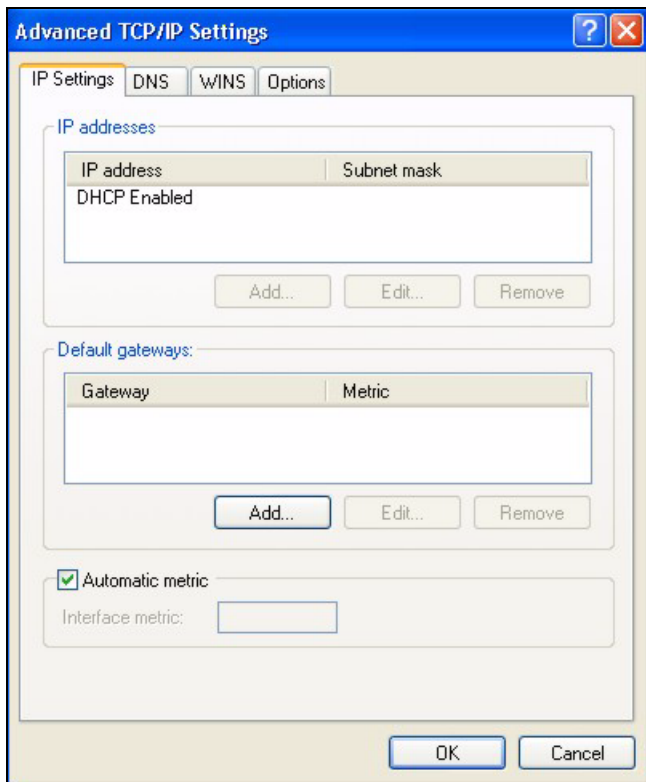
Figure 250 Windows XP: Internet Protocol (TCP/IP) Properties



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

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

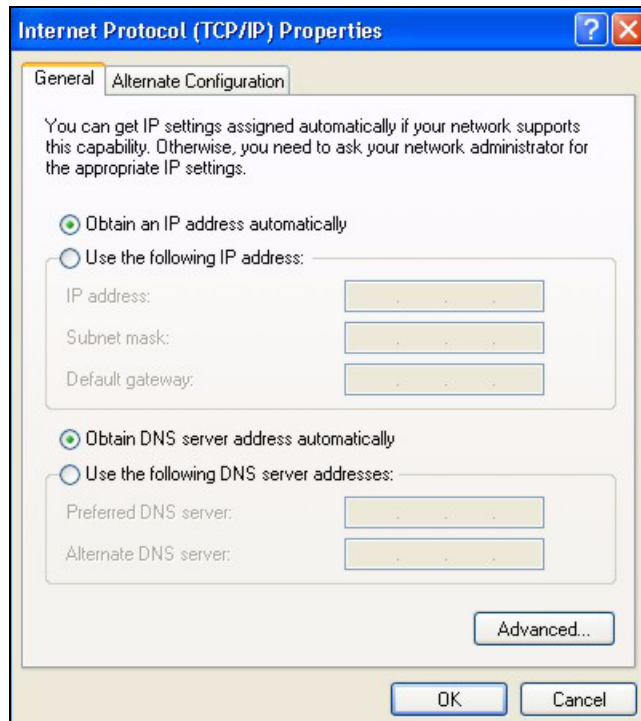
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP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

Figure 251 Windows XP: Advanced TCP/IP Properties

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

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 252 Windows XP: Internet Protocol (TCP/IP) Properties

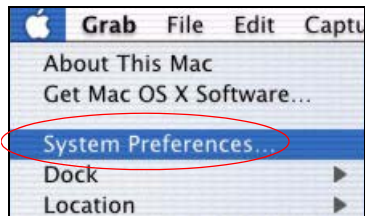
- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.
- 10** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11** Restart 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 X

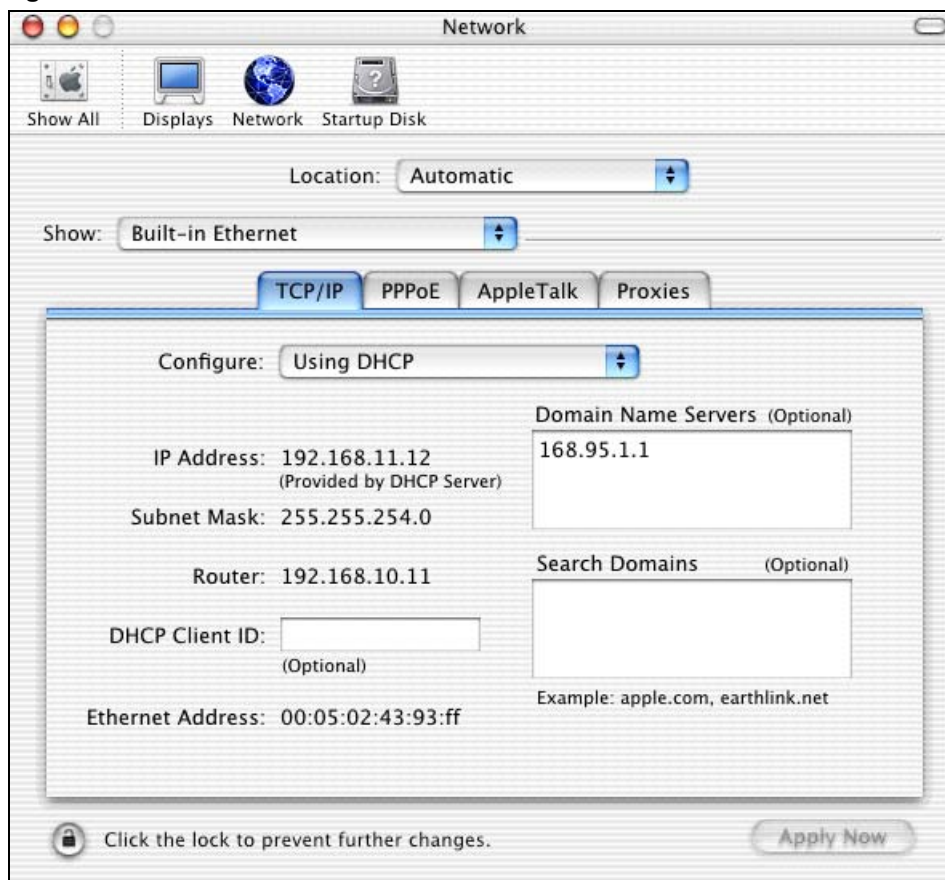
- 1** Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 253 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 254 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 gateway in the **Router address** box.

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

- Restart your computer (if prompted).

Verifying Settings

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

Linux

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

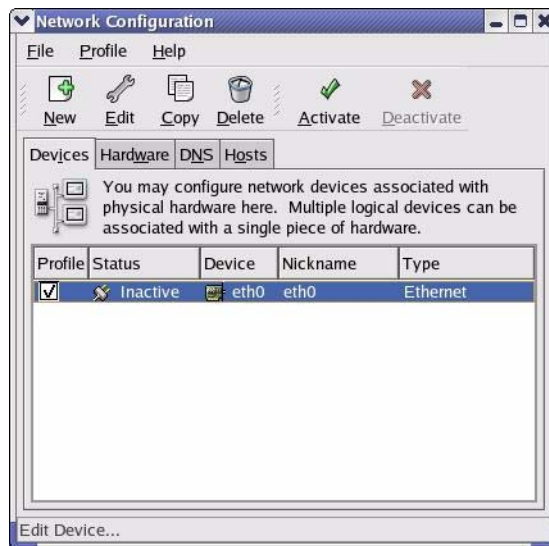
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

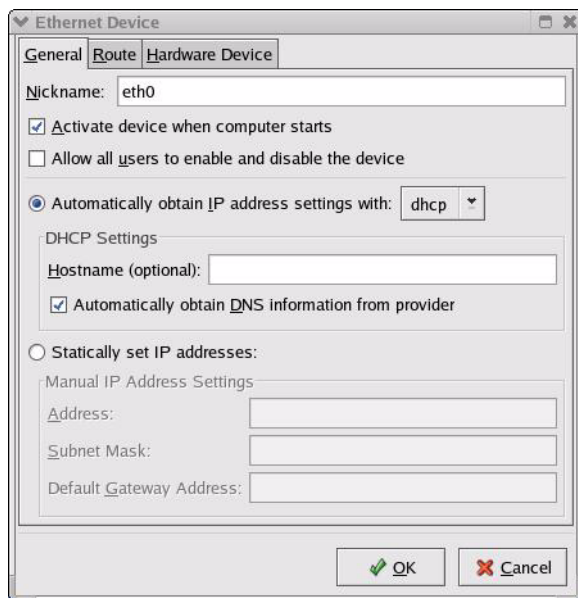
Follow the steps below to configure your computer IP address using the KDE.

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

Figure 255 Red Hat 9.0: KDE: Network Configuration: Devices



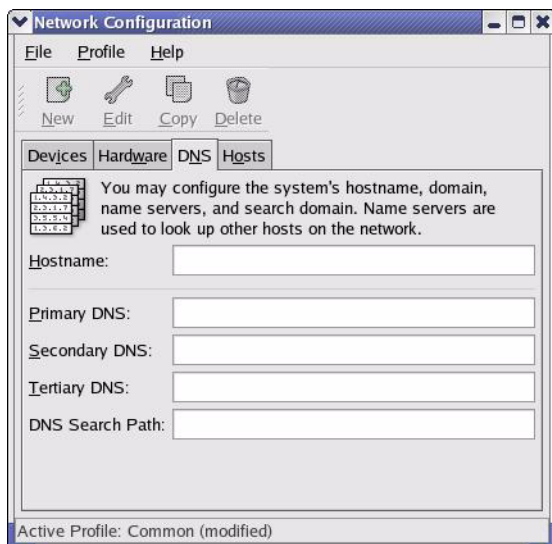
- Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 256 Red Hat 9.0: KDE: Ethernet Device: General

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

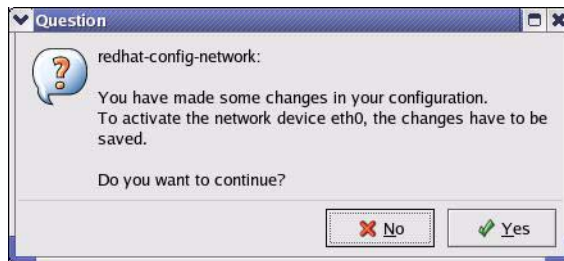
3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

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

Figure 257 Red Hat 9.0: KDE: Network Configuration: DNS

5 Click the **Devices** tab.

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

Figure 258 Red Hat 9.0: KDE: Network Configuration: Activate

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

Using Configuration Files

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

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
 - If you have a dynamic IP address, enter `dhcp` in the `BOOTPROTO=` field. The following figure shows an example.

Figure 259 Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

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

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

Figure 260 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```

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

```

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

Figure 261 Red Hat 9.0: DNS Settings in resolv.conf

```

nameserver 172.23.5.1
nameserver 172.23.5.2

```

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

Figure 262 Red Hat 9.0: Restart Ethernet Card

```

[root@localhost init.d]# network restart

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

```

Verifying Settings

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

Figure 263 Red Hat 9.0: Checking TCP/IP Properties

```

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

```

Appendix C

NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands.

Introduction

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

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

You can configure NetBIOS filters to do the following:

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

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

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

NetBIOS Display Filter Settings Command Example

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

The filter types and their default settings are as follows.

Table 169 NetBIOS Filter Default Settings

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

NetBIOS Filter Configuration

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

where

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

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

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

Example commands

```
sys filter netbios config 0 on    This command blocks LAN to WAN and WAN to LAN NetBIOS packets.
sys filter netbios config 3 on    This command blocks IPSec NetBIOS packets.
sys filter netbios config 4 off   This command stops NetBIOS commands from initiating calls.
```

APPENDIX D

NAT

NAT Overview

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

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 170 NAT Definitions

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

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

What NAT Does

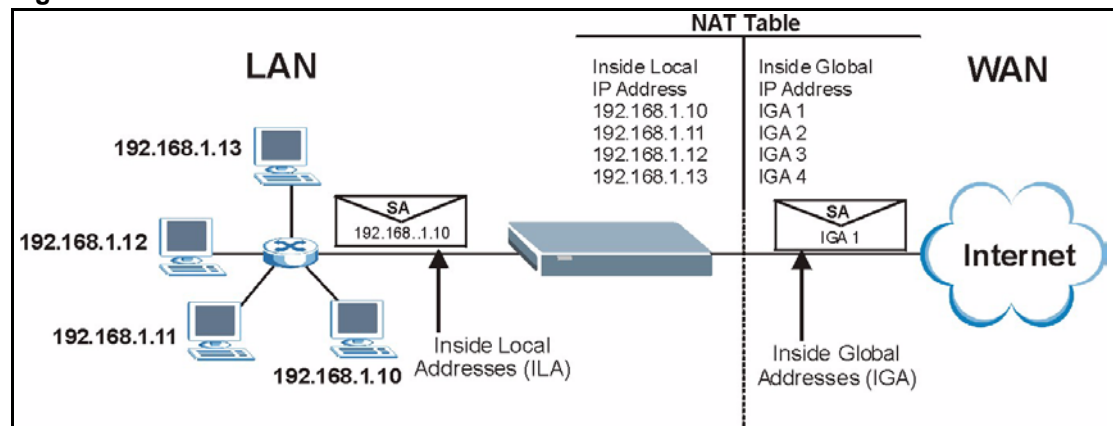
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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), 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)*.

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.

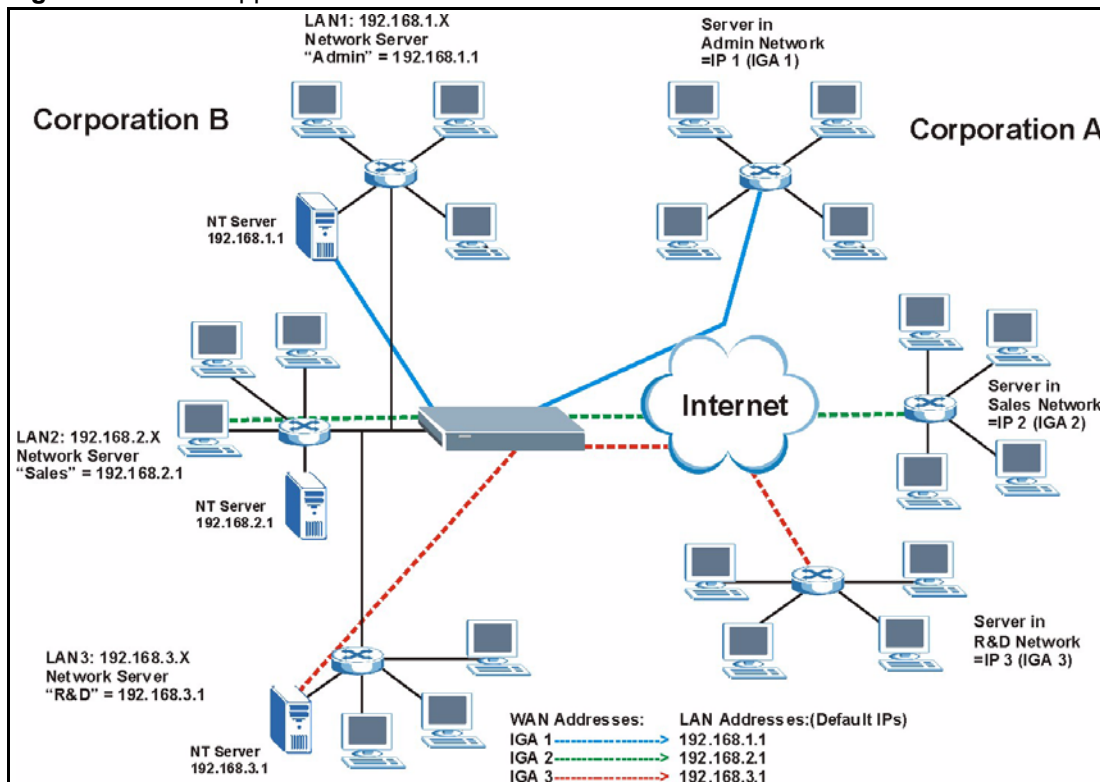
Figure 264 How NAT Works



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 265 NAT Application With IP Alias



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 (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA Only option).
- **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 One-to-One:** In Many-One-to-One mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Note: Port numbers do not change for One-to-One and Many One-to-One NAT mapping types.

The following table summarizes these types.

Table 171 NAT Mapping Types

TYPE	IP MAPPING	ABBREVIATION
One-to-One	ILA1 \leftrightarrow IGA1	1-1
Many-to-One (SUA/PAT)	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA1 ...	M-1
Many-to-Many Overload	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA2 ILA3 \leftrightarrow IGA1 ILA4 \leftrightarrow IGA2 ...	M-M Ov
Many One-to-One	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA2 ILA3 \leftrightarrow IGA3 ...	M-1-1
Server	Server 1 IP \leftrightarrow IGA1 Server 2 IP \leftrightarrow IGA1 Server 3 IP \leftrightarrow IGA1	Server

NAT Types

This section discusses the following NAT types that may be implemented on a router in front of the ZyXEL Device.

- Full Cone
- Restricted Cone
- Port Restricted Cone
- Symmetric

The following table summarizes how these NAT types handle outgoing and incoming packets. Read the following sections for more details and examples.

Table 172 NAT Types

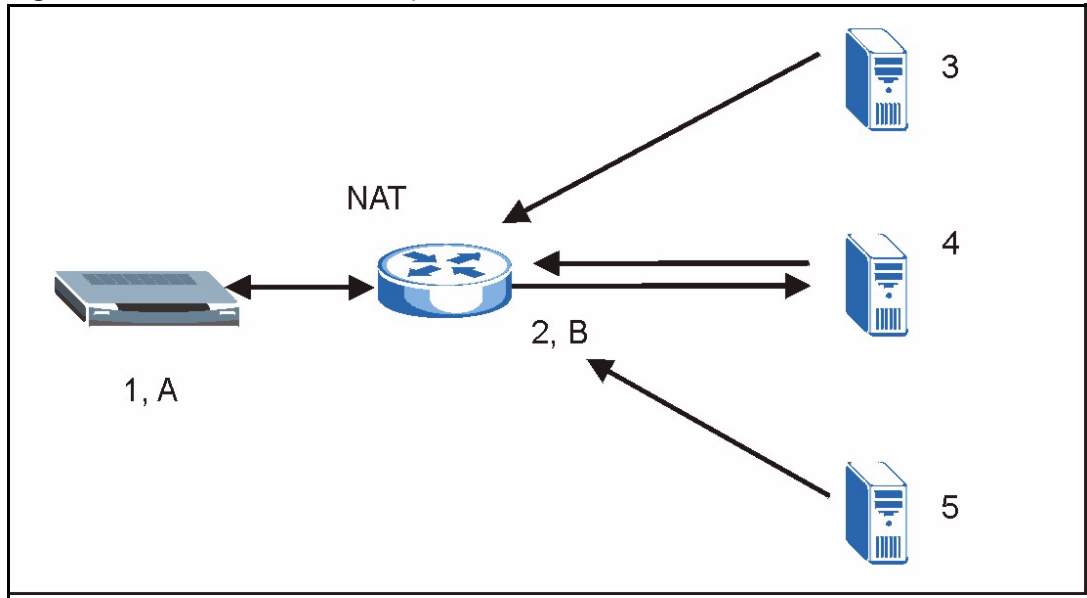
	FULL CONE	RESTRICTED CONE	PORT RESTRICTED CONE	SYMMETRIC
Incoming Packets	Any external host can send packets to the mapped external IP address and port.	Only external hosts with an IP address to which the internal host has already sent a packet can send packets to the mapped external IP address and port.	Only external hosts with an IP address and port to which the internal host has already sent a packet can send packets to the mapped external IP address and port.	A host on the external network can only send packets to the specific mapped external IP address and port that the NAT router used in sending a packet to the external host's IP address and port.
Outgoing Packets	The NAT router maps the internal IP address and port of all outgoing packets to a single IP address and port on the external network.			The NAT router maps the internal IP address and port of each outgoing packet to a different external IP address and port for each different destination IP address and port.

The examples in these NAT type sections describe NAT translation between internal (private) and external (public) IP addresses.

Full Cone NAT

In full cone NAT, the NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The NAT router also maps packets coming to that external IP address and port to the internal IP address and port.

In the following example, the NAT router maps the source address of all packets sent from the ZyXEL Device's internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. The NAT router also performs NAT on all incoming packets sent to IP address **2** and port **B** and sends them to IP address **1**, port **A**.

Figure 266 Full Cone NAT Example

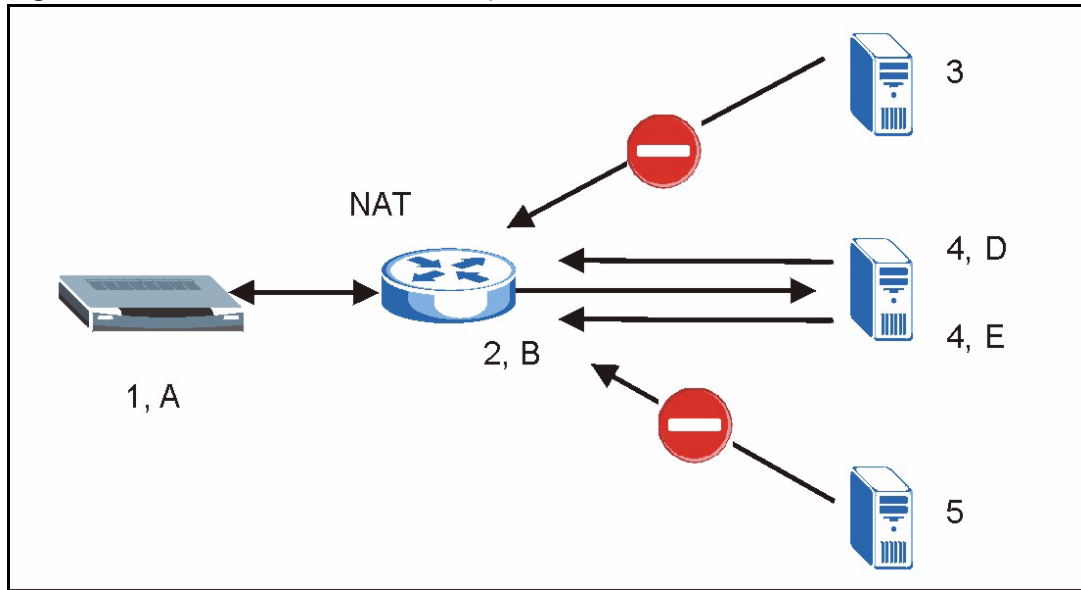
Restricted Cone NAT

As in full cone NAT, a restricted cone NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the NAT router maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network.

The difference from full cone NAT is in how the restricted cone NAT router handles packets coming in from the external network. A host on the external network (IP address **3** or IP address **4** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address.

A ZyXEL Device with IP address **1** and port **A** sends packets to IP address **3** and IP address **4**. The NAT router changes the ZyXEL Device's IP address to **2** and port to **B**.

Both **4, D** and **4, E** can send packets to **2, B** since **1, A** has already sent packets to **4**. The NAT router will perform NAT on the packets from **4, D** and **4, E** and send them to the ZyXEL Device at IP address **1**, port **A**. Packets have not been sent from **1, A** to **3** or **5**, so **3** and **5** cannot send packets to **1, A**.

Figure 267 Restricted Cone NAT Example

Port Restricted Cone NAT

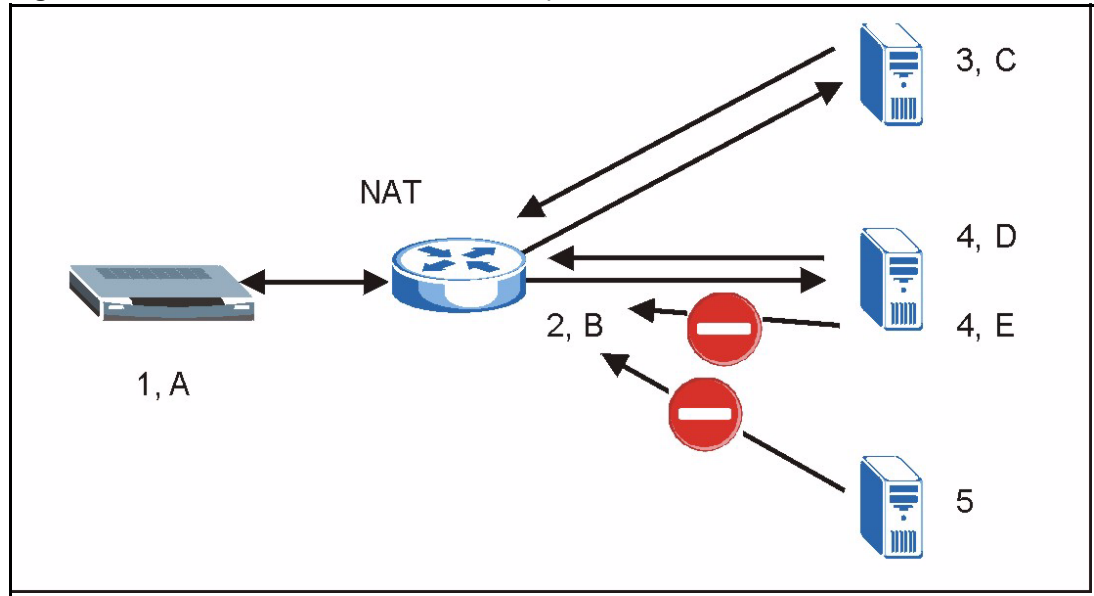
As in full cone NAT, a port restricted cone NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the NAT router maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network.

The difference from full cone and restricted cone NAT is in how the port restricted cone NAT router handles packets coming in from the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A ZyXEL Device with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The NAT router changes the ZyXEL Device's IP address to **2** and port to **B**.

Since **1, A** has already sent packets to **3, C** and **4, D**, they can send packets back to **2, B** and the NAT router will perform NAT on them and send them to the ZyXEL Device at IP address **1**, port **A**.

Packets have not been sent from **1, A** to **4, E** or **5**, so they cannot send packets to **1, A**.

Figure 268 Port Restricted Cone NAT Example

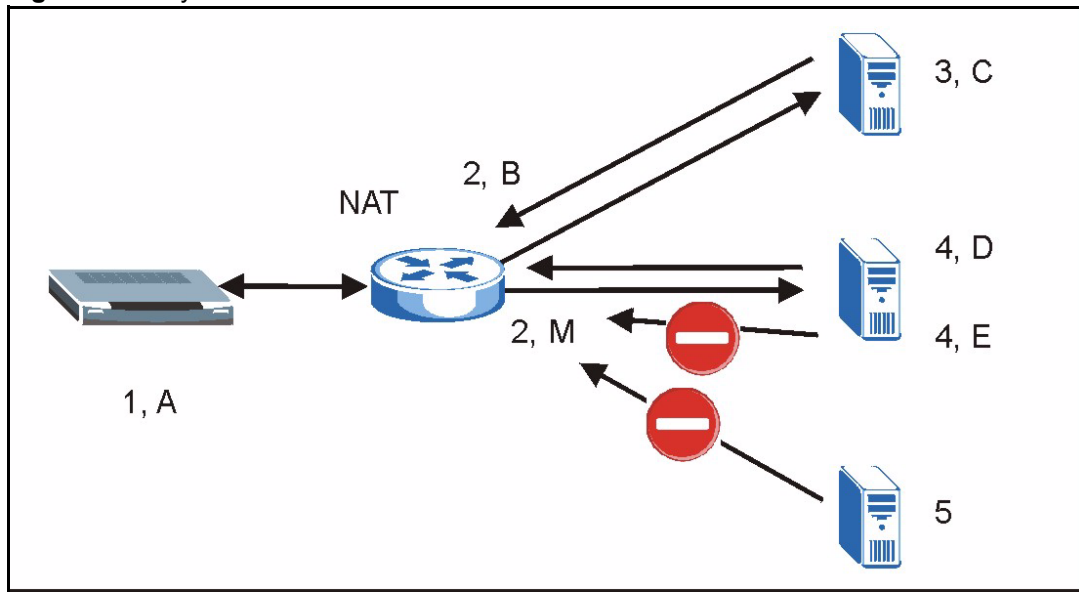
Symmetric NAT

The full, restricted and port restricted cone NAT types use the same mapping for an outgoing packet's source address regardless of the destination IP address and port. In symmetric NAT, the mapping of an outgoing packet's source address to a source address in another network is different for each different destination IP address and port.

In the following example, the NAT router maps the ZyXEL Device's source address IP address **1** and port **A** to IP address **2** and port **B** on the external network for packets sent to IP address **3** and port **B**. The NAT router uses a different mapping (IP address **2** and port **M**) when the ZyXEL Device sends packets to IP address **4** and port **D**.

A host on the external network (IP address **3** and port **C** for example) can only send packets to the internal host via the external IP address and port that the NAT router used in sending a packet to the external host's IP address and port. So in the example, only **3, C** is allowed to send packets to **2, B** and only **4, D** is allowed to send packets to **2, M**.

Figure 269 Symmetric NAT



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.

SUA Server

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

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

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

Appendix E

Firewall Commands

The following describes the firewall commands.

Table 173 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
Firewall SetUp		
	<code>config edit firewall active <yes no></code>	This command turns the firewall on or off.
	<code>config retrieve firewall</code>	This command returns the previously saved firewall settings.
	<code>config save firewall</code>	This command saves the current firewall settings.
Display		
	<code>config display firewall</code>	This command shows the of all the firewall settings including e-mail, attack, and the sets/ rules.
	<code>config display firewall set <set #></code>	This command shows the current configuration of a set; including timeout values, name, default-permit, and etc.If you don't put use a number (#) after "set", information about all of the sets/rules appears.
	<code>config display firewall set <set #> rule <rule #></code>	This command shows the current entries of a rule in a firewall rule set.
	<code>config display firewall attack</code>	This command shows all of the attack response settings.
	<code>config display firewall e-mail</code>	This command shows all of the e-mail settings.
	<code>config display firewall?</code>	This command shows all of the available firewall sub commands.
Edit		
E-mail	<code>config edit firewall e-mail mail-server <ip address of mail server></code>	This command sets the IP address to which the e-mail messages are sent.

Table 173 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	<code>config edit firewall e-mail return-addr <e-mail address></code>	This command sets the source e-mail address of the firewall e-mails.
	<code>config edit firewall e-mail email-to <e-mail address></code>	This command sets the e-mail address to which the firewall e-mails are sent.
	<code>config edit firewall e-mail policy <full hourly daily weekly></code>	This command sets how frequently the firewall log is sent via e-mail.
	<code>config edit firewall e-mail day <sunday monday tuesday wednesday thursday friday saturday></code>	This command sets the day on which the current firewall log is sent through e-mail if the ZyXEL Device is set to send it on a weekly basis.
	<code>config edit firewall e-mail hour <0-23></code>	This command sets the hour when the firewall log is sent through e-mail if the ZyXEL Device is set to send it on an hourly, daily or weekly basis.
	<code>config edit firewall e-mail minute <0-59></code>	This command sets the minute of the hour for the firewall log to be sent via e-mail if the ZyXEL Device is set to send it on a hourly, daily or weekly basis.
Attack	<code>config edit firewall attack send-alert <yes no></code>	This command enables or disables the immediate sending of DOS attack notification e-mail messages.
	<code>config edit firewall attack block <yes no></code>	Set this command to yes to block new traffic after the tcp-max-incomplete threshold is exceeded. Set it to no to delete the oldest half-open session when traffic exceeds the tcp-max-incomplete threshold.
	<code>config edit firewall attack block-minute <0-255></code>	This command sets the number of minutes for new sessions to be blocked when the tcp-max-incomplete threshold is reached. This command is only valid when block is set to yes.
	<code>config edit firewall attack minute-high <0-255></code>	This command sets the threshold rate of new half-open sessions per minute where the ZyXEL Device starts deleting old half-opened sessions until it gets them down to the minute-low threshold.

Table 173 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	<code>config edit firewall attack minute-low <0-255></code>	This command sets the threshold of half-open sessions where the ZyXEL Device stops deleting half-opened sessions.
	<code>config edit firewall attack max-incomplete-high <0-255></code>	This command sets the threshold of half-open sessions where the ZyXEL Device starts deleting old half-opened sessions until it gets them down to the max incomplete low.
	<code>config edit firewall attack max-incomplete-low <0-255></code>	This command sets the threshold where the ZyXEL Device stops deleting half-opened sessions.
	<code>config edit firewall attack tcp-max-incomplete <0-255></code>	This command sets the threshold of half-open TCP sessions with the same destination where the ZyXEL Device starts dropping half-open sessions to that destination.
Sets	<code>config edit firewall set <set #> name <desired name></code>	This command sets a name to identify a specified set.
	<code>Config edit firewall set <set #> default-permit <forward block></code>	This command sets whether a packet is dropped or allowed through, when it does not meet a rule within the set.
	<code>Config edit firewall set <set #> icmp-timeout <seconds></code>	This command sets the time period to allow an ICMP session to wait for the ICMP response.
	<code>Config edit firewall set <set #> udp-idle-timeout <seconds></code>	This command sets how long a UDP connection is allowed to remain inactive before the ZyXEL Device considers the connection closed.
	<code>Config edit firewall set <set #> connection-timeout <seconds></code>	This command sets how long ZyXEL Device waits for a TCP session to be established before dropping the session.
	<code>Config edit firewall set <set #> fin-wait-timeout <seconds></code>	This command sets how long the ZyXEL Device leaves a TCP session open after the firewall detects a FIN-exchange (indicating the end of the TCP session).
	<code>Config edit firewall set <set #> tcp-idle-timeout <seconds></code>	This command sets how long ZyXEL Device lets an inactive TCP connection remain open before considering it closed.

Table 173 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	Config edit firewall set <set #> log <yes no>	This command sets whether or not the ZyXEL Device creates logs for packets that match the firewall's default rule set.
Rules	Config edit firewall set <set #> rule <rule #> permit <forward block>	This command sets whether packets that match this rule are dropped or allowed through.
	Config edit firewall set <set #> rule <rule #> active <yes no>	This command sets whether a rule is enabled or not.
	Config edit firewall set <set #> rule <rule #> protocol <integer protocol value >	This command sets the protocol specification number made in this rule for ICMP.
	Config edit firewall set <set #> rule <rule #> log <none match not-match both>	This command sets the ZyXEL Device to log traffic that matches the rule, doesn't match, both or neither.
	Config edit firewall set <set #> rule <rule #> alert <yes no>	This command sets whether or not the ZyXEL Device sends an alert e-mail when a DOS attack or a violation of a particular rule occurs.
	config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>	This command sets the rule to have the ZyXEL Device check for traffic with this individual source address.
	config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>	This command sets a rule to have the ZyXEL Device check for traffic from a particular subnet (defined by IP address and subnet mask).
	config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>	This command sets a rule to have the ZyXEL Device check for traffic from this range of addresses.
	config edit firewall set <set #> rule <rule #> destaddr-single <ip address>	This command sets the rule to have the ZyXEL Device check for traffic with this individual destination address.

Table 173 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	<code>config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask></code>	This command sets a rule to have the ZyXEL Device check for traffic with a particular subnet destination (defined by IP address and subnet mask).
	<code>config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address></code>	This command sets a rule to have the ZyXEL Device check for traffic going to this range of addresses.
	<code>config edit firewall set <set #> rule <rule #> TCP destport-single <port #></code>	This command sets a rule to have the ZyXEL Device check for TCP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	<code>config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #></code>	This command sets a rule to have the ZyXEL Device check for TCP traffic with a destination port in this range.
	<code>config edit firewall set <set #> rule <rule #> UDP destport-single <port #></code>	This command sets a rule to have the ZyXEL Device check for UDP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	<code>config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #></code>	This command sets a rule to have the ZyXEL Device check for UDP traffic with a destination port in this range.
Delete		
	<code>config delete firewall e-mail</code>	This command removes all of the settings for e-mail alert.
	<code>config delete firewall attack</code>	This command resets all of the attack response settings to their defaults.
	<code>config delete firewall set <set #></code>	This command removes the specified set from the firewall configuration.
	<code>config delete firewall set <set #> rule<rule #></code>	This command removes the specified rule in a firewall configuration set.

Appendix F

Log Descriptions

This appendix provides descriptions of example log messages.

Table 174 System Maintenance Logs

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

Table 174 System Maintenance Logs (continued)

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

Table 175 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 176 Access Control Logs

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

Table 177 TCP Reset Logs

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

Table 178 Packet Filter Logs

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

Table 179 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. For type and code details, see Table 191 on page 409 .
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 191 on page 409 .
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 180 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 181 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 181 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 182 UPnP Logs

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

Table 183 Content Filtering Logs

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

Table 183 Content Filtering Logs (continued)

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

Table 184 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. For type and code details, see Table 191 on page 409 .
land [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack. For type and code details, see Table 191 on page 409 .
ip spoofing - WAN [TCP UDP IGMP ESP GRE OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 191 on page 409 .
icmp echo: ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 191 on page 409 .
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack. For type and code details, see Table 191 on page 409 .
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP UDP IGMP ESP GRE OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 191 on page 409 .
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack. For type and code details, see Table 191 on page 409 .

Table 185 IPsec Logs

LOG MESSAGE	DESCRIPTION
Discard REPLAY packet	The router received and discarded a packet with an incorrect sequence number.
Inbound packet authentication failed	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
Receive IPsec packet, but no corresponding tunnel exists	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
Rule <%d> idle time out, disconnect	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CLI command to set the time period. The default value is 2 minutes.
WAN IP changed to <IP>	The router dropped all connections with the "MyIP" configured as "0.0.0.0" when the WAN IP address changed.

Table 186 IKE Logs

LOG MESSAGE	DESCRIPTION
Active connection allowed exceeded	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
Start Phase 2: Quick Mode	Phase 2 Quick Mode has started.
Verifying Remote ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
Verifying Local ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
IKE Packet Retransmit	The router retransmitted the last packet sent because there was no response from the peer.
Failed to send IKE Packet	An Ethernet error stopped the router from sending IKE packets.
Too many errors! Deleting SA	An SA was deleted because there were too many errors.
Phase 1 IKE SA process done	The phase 1 IKE SA process has been completed.
Duplicate requests with the same cookie	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
IKE Negotiation is in process	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
No proposal chosen	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
Local / remote IPs of incoming request conflict with rule <%d>	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.

Table 186 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Cannot resolve Secure Gateway Addr for rule <%d>	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
Peer ID: <peer id> <My remote type> -<My local type>	The displayed ID information did not match between the two ends of the connection.
vs. My Remote <My remote> - <My remote>	The displayed ID information did not match between the two ends of the connection.
vs. My Local <My local>-<My local>	The displayed ID information did not match between the two ends of the connection.
Send <packet>	A packet was sent.
Recv <packet>	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
Recv <Main or Aggressive> Mode request from <IP>	The router received an IKE negotiation request from the peer address specified.
Send <Main or Aggressive> Mode request to <IP>	The router started negotiation with the peer.
Invalid IP <Peer local> / <Peer local>	The peer's "Local IP Address" is invalid.
Remote IP <Remote IP> / <Remote IP> conflicts	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Phase 1 ID type mismatch	This router's "Peer ID Type" is different from the peer IPsec router's "Local ID Type".
Phase 1 ID content mismatch	This router's "Peer ID Content" is different from the peer IPsec router's "Local ID Content".
No known phase 1 ID type found	The router could not find a known phase 1 ID in the connection attempt.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	The phase 1 ID types do not match.
ID content mismatch	The phase 1 ID contents do not match.
Configured Peer ID Content: <Configured Peer ID Content>	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
Incoming ID Content: <Incoming Peer ID Content>	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
Unsupported local ID Type: <%d>	The phase 1 ID type is not supported by the router.
Build Phase 1 ID	The router has started to build the phase 1 ID.
Adjust TCP MSS to%d	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
Rule <%d> input idle time out, disconnect	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
XAUTH succeed! Username: <Username>	The router used extended authentication to authenticate the listed username.

Table 186 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed username.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication algorithm mismatch	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication method mismatch	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
Rule [%d] Phase 1 key group mismatch	The listed rule's IKE phase 1 key group did not match between the router and the peer.
Rule [%d] Phase 2 protocol mismatch	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
Rule [%d] Phase 2 encryption algorithm mismatch	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 2 authentication algorithm mismatch	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 2 encapsulation mismatch	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
Rule [%d]> Phase 2 pfs mismatch	The listed rule's IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.
Rule [%d] Phase 1 ID mismatch	The listed rule's IKE phase 1 ID did not match between the router and the peer.
Rule [%d] Phase 1 hash mismatch	The listed rule's IKE phase 1 hash did not match between the router and the peer.
Rule [%d] Phase 1 preshared key mismatch	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
Rule [%d] Tunnel built successfully	The listed rule's IPsec tunnel has been built successfully.
Rule [%d] Peer's public key not found	The listed rule's IKE phase 1 peer's public key was not found.
Rule [%d] Verify peer's signature failed	The listed rule's IKE phase 1 verification of the peer's signature failed.
Rule [%d] Sending IKE request	IKE sent an IKE request for the listed rule.
Rule [%d] Receiving IKE request	IKE received an IKE request for the listed rule.
Swap rule to rule [%d]	The router changed to using the listed rule.
Rule [%d] Phase 1 key length mismatch	The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
Rule [%d] phase 1 mismatch	The listed rule's IKE phase 1 did not match between the router and the peer.

Table 186 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] phase 2 mismatch	The listed rule's IKE phase 2 did not match between the router and the peer.
Rule [%d] Phase 2 key length mismatch	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.

Table 187 PKI Logs

LOG MESSAGE	DESCRIPTION
Enrollment successful	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
Enrollment failed	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <SCEP CA server url>	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
Enrollment successful	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
Enrollment failed	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <CMP CA server url>	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
Rcvd ca cert: <subject name>	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd user cert: <subject name>	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd CRL <size>: <issuer name>	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd ARL <size>: <issuer name>	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ca cert	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received user cert	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received CRL	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ARL	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.

Table 187 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Rcvd data <size> too large! Max size allowed: <max size>	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
Cert trusted: <subject name>	The router has verified the path of the certificate with the listed subject name.
Due to <reason codes>, cert not trusted: <subject name>	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 188 on page 407 for the corresponding descriptions of the codes.

Table 188 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.

Table 188 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 189 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication method.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 190 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/ZW)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W/ZW)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.

Table 191 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 191 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 192 Syslog Logs

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

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

Table 193 RFC-2408 ISAKMP Payload Types

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

Log Commands

Go to the command interpreter interface.

Configuring What You Want the ZyXEL Device to Log

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

Figure 270 Displaying Log Categories Example

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras>?
Valid commands are:
sys          exit          ether          aux
ip           ipsec          bridge         bm
certificates cnm           8021x         radius
ras>
```

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

Figure 271 Displaying Log Parameters Example

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

- 4 Use `sys logs category` followed by a log category and a parameter to decide what to record.

Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.

- 5 Step 5. Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

Displaying Logs

- Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.

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

Log Command Example

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

```

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

```

#.time	source	destination	notes
message			
0 06/08/2004 05:58:21	172.21.4.154	224.0.1.24	ACCESS
BLOCK			
Firewall default policy: IGMP (W to W/ZW)			
1 06/08/2004 05:58:20	172.21.3.56	239.255.255.250	ACCESS
BLOCK			
Firewall default policy: IGMP (W to W/ZW)			
2 06/08/2004 05:58:20	172.21.0.2	239.255.255.254	ACCESS
BLOCK			
Firewall default policy: IGMP (W to W/ZW)			
3 06/08/2004 05:58:20	172.21.3.191	224.0.1.22	ACCESS
BLOCK			
Firewall default policy: IGMP (W to W/ZW)			
4 06/08/2004 05:58:20	172.21.0.254	224.0.0.1	ACCESS
BLOCK			
Firewall default policy: IGMP (W to W/ZW)			
5 06/08/2004 05:58:20	172.21.4.187:137	172.21.255.255:137	ACCESS
BLOCK			
Firewall default policy: UDP (W to W/ZW)			

Appendix G

Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware is started. When you start up your ZyXEL Device, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the **Firmware and Configuration File Maintenance** chapter.

Figure 272 Option to Enter Debug Mode

```
Bootbase Version: V1.02 | 08/08/2001 15:40:50
RAM: Size = 16384 Kbytes
DRAM Post: Testing: 16384K OK
FLASH: Intel 16M
RAS Version: V3.50(WB.0)b3 | 08/08/2001 16:21:27
Press any key to enter debug mode within 3
seconds.
.....
```

Enter ATHE to view all available ZyXEL Device boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

Figure 273 Boot Module Commands

AT	just answer OK
ATHE	print help
ATBAx	change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k
5:115.2k	
ATENx, (y)	set BootExtension Debug Flag (y=password)
ATSE	show the seed of password generator
ATTI(h,m,s)	change system time to hour:min:sec or show
current time	
ATDA(y,m,d)	change system date to year/month/day or show
current date	
ATDS	dump RAS stack
ATDT	dump Boot Module Common Area
ATDUx,y	dump memory contents from address x for length y
ATRBx	display the 8-bit value of address x
ATRWx	display the 16-bit value of address x
ATRLx	display the 32-bit value of address x
ATGO(x)	run program at addr x or boot router
ATGR	boot router
ATGT	run Hardware Test Program
ATRTw,x,y(,z)	RAM test level w, from address x to y (z
iterations)	
ATSH	dump manufacturer related data in ROM
ATDOx,y	download from address x for length y to PC via
XMODEM	
ATTD	download router configuration to PC via XMODEM
ATUR	upload router firmware to flash ROM
ATLC	upload router configuration file to flash ROM
ATXSx	xmodem select: x=0: CRC mode(default); x=1:
checksum mode	
ATSR	system reboot

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 274 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 274 on page 415](#)), 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 275 on page 416](#), 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 274 on page 415](#)).

Figure 275 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 276 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 277 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.
- 4 Exit this FTP application.

Figure 278 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 194 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 195 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 196 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 196 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 196 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 196 Menu 3

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

Table 197 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 (D ynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0 (No) 1 (Yes)>	= 1
40000026 =	Bridge	<0 (No) 1 (Yes)>	= 0

Table 197 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 198 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 199 Menu 15 SUA Server Setup

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

Table 199 Menu 15 SUA Server Setup (continued)

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

Table 200 Menu 21.1 Filter Set #1

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

Table 200 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 200 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 201 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 201 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 202 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 202 Menu 23 System Menus (continued)

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

Table 203 Menu 24.11 Remote Management Control

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

Table 203 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

Appendix I

Services

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

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

Table 204 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

Table 204 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.

Table 204 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.

Index

A

access point. See AP.
AP [93](#)

B

backup [320](#)
bandwidth management [41, 197](#)
bandwidth manager class configuration [202](#)
bandwidth manager monitor [204](#)
blocking time [151, 164](#)

C

call control [333, 334](#)
call scheduling [347](#)
 precedence [348](#)
 precedence example [348](#)
certifications [4](#)
 notices [5](#)
 viewing [5](#)
change password at login [48, 49](#)
channel [93, 97](#)
CI commands [333](#)
Command Interpreter (CI) [333](#)
computer's IP address [365](#)
configuration
 back up [243](#)
 reset to factory defaults [243](#)
 restore [243](#)
contact information [9](#)
content filtering [40](#)
copyright [3](#)
custom ports
 creating/editing [160](#)
customer support [9](#)
customized services [160](#)

D

default LAN IP address [47](#)
Denial of Service. See DoS.
device model number [241](#)
DHCP [41, 229](#)
DHCP client [41](#)
DHCP relay [41](#)
DHCP server [41](#)
dial-in user setup [277](#)
disclaimer [3](#)
DoS [40, 147, 150, 151](#)
dynamic DNS [41, 229](#)
Dynamic Host Configuration Protocol. See DHCP.
DYNDNS wildcard [230](#)

E

embedded help [50](#)
encryption [95](#)
 key [96](#)
 types of [95](#)
 WPA compatible [96](#)
Ethernet encapsulation [137](#)

F

FCC interference statement [4](#)
filename conventions [319](#)
filters [287](#)
 applying [300](#)
 example [297](#)
 generic filter rule [295](#)
 NAT [300](#)
 remote node [301](#)
 structure [288](#)
firewall
 address type [159](#)
 anti-probing [161](#)
 creating/editing rules [157](#)
 custom ports [160](#)
 enabling [154](#)

- guidelines for enhancing security [153](#)
- introduction [147](#)
- policies [148](#)
- rule checklist [149](#)
- rule logic [149](#)
- rule security ramifications [149](#)
- services [149](#)

firewall setup [305](#)

firmware [241](#)

- upgrade [241](#)
- upload [241](#)
- upload error [242](#), [244](#)

FTP [205](#), [389](#)

FTP file transfer [326](#)

FTP restrictions [205](#)

full cone NAT [385](#)

G

general setup [229](#), [253](#)

H

half-open sessions [150](#)

hidden menus [251](#)

hide SSID [94](#)

host [231](#)

HTTP [241](#)

HyperTerminal [324](#)

Hypertext Transfer Protocol. See HTTP.

I

idle timeout [206](#)

IEEE 802.11g [41](#)

IEEE 802.11i [42](#)

IGMP [128](#)

inside global address (IGA) [381](#)

inside local address (ILA) [381](#)

Internet access [39](#)

Internet access setup [267](#)

Internet Assigned Number Authority (IANA) [160](#)

Internet Group Multicast Protocol. See IGMP.

IP address [127](#)

IP alias [41](#), [383](#)

- and NAT [383](#)

IP pool [134](#)

IP protocol type [150](#)

IP Routing Policy. See IPPR.

IPPR [339](#)

- benefits [339](#)
- cost savings [339](#)
- criteria [339](#)
- load sharing [339](#)

L

LAN setup [127](#), [133](#), [259](#)

local (user) database [95](#)

logs [237](#)

M

MAC address [94](#)

MAC address filter [94](#)

- action [112](#)
- weaknesses [94](#)

main menu [247](#)

Management Information Base (MIB) [207](#)

mapping

- NAT, many one-to-one [383](#)
- NAT, many-to-many overload [383](#)
- NAT, many-to-one [383](#)
- NAT, one-to-one [383](#)
- NAT, server [383](#)

max-incomplete high [151](#)

max-incomplete low [151](#)

metric [119](#)

multicast [128](#)

N

nailed-up connection [119](#)

NAT [40](#), [300](#), [381](#), [389](#)

- and IP alias [383](#)
- and remote management [206](#)
- application [383](#)
- definitions [381](#)
- full cone [385](#)
- global [381](#)
- how NAT works [382](#)
- inside [381](#)
- local [381](#)

- mapping types [383](#)
- outside [381](#)
- port forwarding [137](#)
- server sets [137](#)
- symmetric [388](#)
- what NAT does [382](#)
- NAT mapping [383](#)
 - many one-to-one [383](#)
 - many-to-many overload [383](#)
 - many-to-one [383](#)
 - server [383](#)
- NAT setup [279](#)
- NAT traversal [217](#)
- NAT types [389](#)
- Network Address Translation. See NAT.

O

- one-minute high [151](#)
- OTIST [96](#)
 - notes [111](#)

P

- password [232](#), [247](#), [254](#)
- Point-to-Point Protocol over Ethernet. See PPPoE.
- policy-based routing [339](#)
- port forwarding [137](#)
- port numbers [137](#)
- port restricted cone NAT [387](#)
- PPPoE [40](#)
- priorities [197](#)
- priority-based scheduler [197](#)
- product registration [8](#)

Q

- QoS [39](#), [96](#)
 - benefits [96](#)
- Quality of Service. See QoS
- Quick Start Guide [37](#)

R

- radio frequency [42](#)
- RADIUS server [95](#)
- RAS [340](#)
- registration
 - product [8](#)
- related documentation [37](#)
- remote management [205](#)
 - and NAT [206](#)
 - limitations [205](#)
- remote node setup [269](#)
- required fields [252](#)
- restore configuration [324](#)
- restricted cone NAT [386](#)
- RFC 1213 [207](#)
- RFC 1215 [207](#)
- RFC 1631. See NAT.
- RFC 2516. See PPPoE.
- RIP [127](#)
 - direction [127](#)
 - version [128](#)
- Routing Information Protocol. See RIP.
- routing policy [339](#)
- rules
 - checklist [149](#)
 - logic [149](#)
 - predefined services [149](#)

S

- safety warnings [6](#)
- schedule setup [347](#)
- security in general [153](#)
- security ramifications [149](#)
- Service Set IDentity. See SSID.
- service type [161](#)
- services [137](#)
- Simple Network Management Protocol. See SNMP.
- Single User Account. See SUA.
- SMT [247](#)
- SMT menu overview [248](#)
- SNMP [206](#)
 - Get [207](#)
 - GetNext [207](#)
 - manager [207](#)
 - MIBs [207](#)
 - Set [207](#)
 - Trap [207](#)
 - trusted host [307](#)

SNMPv1 [206](#)
SNMPv2 [206](#)
source-based routing [339](#)
splitters [44](#)
SPTGEN [415](#)
 FTP upload example [417](#)
 points to remember [416](#)
 text file [415](#)
SSID [93, 94](#)
 hide [94](#)
SSID security [94](#)
 weaknesses [94](#)
stateful inspection [40, 147](#)
static routing setup [275](#)
SUA [389](#)
SUA server set [389](#)
subnet mask [127, 159](#)
supporting disk [37](#)
symmetric NAT [388](#)
 outgoing [389](#)
syntax conventions [37](#)
system maintenance [320, 322, 324, 325, 328, 329](#)
System Management Terminal. See SMT.
system name [230](#)
System Parameter Table Generator. See SPTGEN.
system timeout [206](#)

T

TCP Maximum Incomplete [151](#)
TCP/IP filter rule [292](#)
text file format [415](#)
TFTP file transfer [328](#)
TFTP restrictions [205](#)
threshold values [150](#)
time server [234, 336](#)
TMM QoS. See also QoS.
trademarks [3](#)
traffic redirect [40](#)
triangle route [152](#)
 solutions [152](#)
trigger port forwarding [138](#)
 process [138](#)
Triple Play [39](#)

U

Universal Plug and Play. See UPnP.
upload firmware [325](#)
UPnP [41, 217](#)
 applications [217](#)
 Forum [218](#)
 installation [219](#)
 installation, Windows Me [219](#)
 installation, Windows XP [220](#)
 security issues [217](#)
user authentication [94](#)
 local (user) database [95](#)
 RADIUS server [95](#)
 weaknesses [95](#)
user name [232, 254](#)

W

WAN setup [257](#)
warranty [8](#)
 note [8](#)
web configurator [47, 49, 149, 153](#)
web configurator screen summary [50](#)
WEP encryption [63, 65](#)
Wi-Fi Protected Access. See WPA.
wireless
 MAC address filtering [42](#)
wireless client [93](#)
wireless network [93](#)
 basic guidelines [93](#)
wireless networks
 channel [93](#)
 encryption [95](#)
 MAC address filter [94](#)
 OTIST [96](#)
 security [94](#)
 SSID [93](#)
 user authentication [94](#)
wireless security [94](#)
WPA [42](#)
WPA compatible [96](#)

Z

ZyNOS [320](#)
ZyNOS firmware version [320](#)