

# *P-2608HWL-Dx Series*

*802.11g Wireless ADSL2+ VoIP IAD*

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

Version 3.40

10/2006

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 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

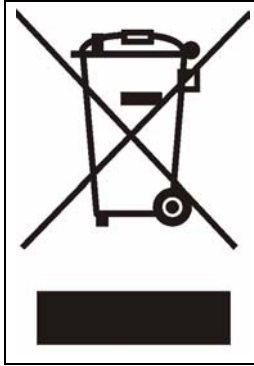
- 1 Go to <http://www.zyxel.com>.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

# Safety Warnings

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

- Do NOT 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.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- To reduce the risk of fire, 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](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://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 Česká 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, Zoldomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	

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

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

# Table of Contents

<b>Copyright</b> .....	<b>3</b>
<b>Certifications</b> .....	<b>4</b>
<b>Safety Warnings</b> .....	<b>6</b>
<b>ZyXEL Limited Warranty</b> .....	<b>8</b>
<b>Customer Support</b> .....	<b>9</b>
<b>Table of Contents</b> .....	<b>11</b>
<b>List of Figures</b> .....	<b>25</b>
<b>List of Tables</b> .....	<b>33</b>
<b>Preface</b> .....	<b>39</b>
<b>Chapter 1</b>	
<b>Getting To Know the ZyXEL Device</b> .....	<b>41</b>
1.1 Overview .....	41
1.1.1 VoIP Features .....	41
1.1.2 DSL Router .....	42
1.2 LEDs (Lights) .....	42
<b>Chapter 2</b>	
<b>Introducing the Web Configurator</b> .....	<b>45</b>
2.1 Web Configurator Overview .....	45
2.1.1 Accessing the Web Configurator .....	45
2.1.2 The RESET Button .....	48
2.1.2.1 Using The Reset Button .....	48
2.2 Web Configurator Main Screen .....	48
2.2.1 Title Bar .....	49
2.2.2 Navigation Panel .....	49
2.2.3 Status Bar .....	52
<b>Chapter 3</b>	
<b>Internet and Wireless Setup Wizard</b> .....	<b>53</b>
3.1 Introduction .....	53
3.2 Internet Access Wizard Setup .....	53
3.2.1 Manual Configuration .....	55

3.3 Wireless Connection Wizard Setup .....	60
3.3.1 Automatically assign a WPA key .....	63
3.3.2 Manually Assign a WPA key .....	63
3.3.3 Manually Assign a WEP key .....	63
<b>Chapter 4</b>	
<b>VoIP Wizard And Example .....</b>	<b>67</b>
4.1 Introduction .....	67
4.2 VoIP Wizard Setup .....	67
<b>Chapter 5</b>	
<b>Bandwidth Management Wizard .....</b>	<b>73</b>
5.1 Introduction .....	73
5.2 Predefined Media Bandwidth Management Services .....	73
5.3 Bandwidth Management Wizard Setup .....	74
<b>Chapter 6</b>	
<b>Status Screens .....</b>	<b>79</b>
6.1 Status Screen .....	79
6.2 Any IP Table .....	82
6.3 WLAN Status .....	83
6.4 Packet Statistics .....	83
6.5 VoIP Statistics .....	85
<b>Chapter 7</b>	
<b>WAN Setup .....</b>	<b>89</b>
7.1 WAN Overview .....	89
7.1.1 Encapsulation .....	89
7.1.1.1 ENET ENCAP .....	89
7.1.1.2 PPP over Ethernet .....	89
7.1.1.3 PPPoA .....	90
7.1.1.4 RFC 1483 .....	90
7.1.2 Multiplexing .....	90
7.1.2.1 VC-based Multiplexing .....	90
7.1.2.2 LLC-based Multiplexing .....	90
7.1.3 VPI and VCI .....	90
7.1.4 IP Address Assignment .....	91
7.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation .....	91
7.1.4.2 IP Assignment with RFC 1483 Encapsulation .....	91
7.1.4.3 IP Assignment with ENET ENCAP Encapsulation .....	91
7.1.5 Nailed-Up Connection (PPP) .....	91
7.1.6 NAT .....	91
7.2 Metric .....	92



7.3 Traffic Shaping .....	92
7.3.1 ATM Traffic Classes .....	93
7.3.1.1 Constant Bit Rate (CBR) .....	93
7.3.1.2 Variable Bit Rate (VBR) .....	93
7.3.1.3 Unspecified Bit Rate (UBR) .....	94
7.4 Zero Configuration Internet Access .....	94
7.5 Internet Access Setup .....	94
7.5.1 Advanced Internet Access Setup.....	97
7.6 WAN More Connections .....	98
7.6.1 WAN More Connections Modify Screen .....	99
7.7 Traffic Redirect .....	102
7.8 WAN Backup Setup .....	103

## Chapter 8

### LAN Setup..... 105

8.1 LAN Overview .....	105
8.1.1 LANs, WANs and the ZyXEL Device .....	105
8.1.2 DHCP Setup .....	106
8.1.2.1 IP Pool Setup .....	106
8.1.3 DNS Server Address .....	106
8.1.4 DNS Server Address Assignment .....	107
8.2 LAN TCP/IP .....	107
8.2.1 IP Address and Subnet Mask .....	107
8.2.1.1 Private IP Addresses .....	108
8.2.2 RIP Setup .....	108
8.2.3 Multicast .....	109
8.2.4 Any IP .....	109
8.2.4.1 How Any IP Works .....	110
8.3 Configuring LAN IP .....	111
8.3.1 Configuring Advanced LAN Setup.....	111
8.4 DHCP Setup .....	113
8.5 LAN Client List .....	114
8.6 LAN IP Alias .....	115

## Chapter 9

### Wireless LAN..... 119

9.1 Wireless Network Overview .....	119
9.2 Wireless Security Overview .....	120
9.2.1 SSID .....	120
9.2.2 MAC Address Filter .....	120
9.2.3 User Authentication .....	120
9.2.4 Encryption .....	121
9.2.5 One-Touch Intelligent Security Technology (OTIST) .....	122

9.3 Wireless Performance Overview .....	122
9.3.1 Quality of Service (QoS) .....	122
9.4 Additional Wireless Terms .....	122
9.5 General Wireless LAN Screen .....	123
9.5.1 No Security .....	124
9.5.2 WEP Encryption Screen .....	125
9.5.3 WPA(2)-PSK .....	126
9.5.4 WPA(2) Authentication Screen .....	128
9.5.5 Wireless LAN Advanced Setup.....	129
9.6 OTIST Screen .....	130
9.6.1 Notes on OTIST .....	133
9.7 MAC Filter .....	134
9.8 QoS Screen .....	135
9.8.1 Application Priority Configuration.....	136
<b>Chapter 10</b>	
<b>Network Address Translation (NAT) Screens .....</b>	<b>139</b>
10.1 NAT Overview .....	139
10.1.1 NAT Definitions .....	139
10.1.2 What NAT Does .....	140
10.1.3 How NAT Works .....	140
10.1.4 NAT Application .....	141
10.1.5 NAT Mapping Types .....	141
10.2 SUA (Single User Account) Versus NAT .....	142
10.3 NAT General Setup .....	142
10.4 Port Forwarding .....	143
10.4.1 Default Server IP Address .....	144
10.4.2 Port Forwarding: Services and Port Numbers .....	144
10.4.3 Configuring Servers Behind Port Forwarding (Example) .....	144
10.5 Configuring Port Forwarding .....	145
10.5.1 Port Forwarding Rule Edit .....	146
10.6 Address Mapping .....	147
10.6.1 Address Mapping Rule Edit .....	148
10.6.2 SIP ALG .....	149
<b>Chapter 11</b>	
<b>SIP .....</b>	<b>151</b>
11.1 SIP Overview .....	151
11.1.1 Introduction to VoIP .....	151
11.1.2 Introduction to SIP .....	151
11.1.3 SIP Identities .....	151
11.1.3.1 SIP Number .....	151
11.1.3.2 SIP Service Domain .....	152

11.1.4 SIP Call Progression .....	152
11.1.5 SIP Client Server .....	152
11.1.5.1 SIP User Agent .....	153
11.1.5.2 SIP Proxy Server .....	153
11.1.5.3 SIP Redirect Server .....	154
11.1.5.4 SIP Register Server .....	154
11.1.6 RTP .....	154
11.1.7 NAT and SIP .....	155
11.1.7.1 SIP ALG .....	155
11.1.7.2 Use NAT .....	155
11.1.7.3 STUN .....	155
11.1.7.4 Outbound Proxy .....	156
11.1.8 Voice Coding .....	156
11.1.9 PSTN Call Setup Signaling .....	156
11.1.10 MWI (Message Waiting Indication) .....	157
11.1.11 Custom Tones (IVR) .....	157
11.1.11.1 Recording Custom Tones .....	157
11.1.11.2 Listening to Custom Tones .....	157
11.1.11.3 Deleting Custom Tones .....	157
11.1.12 Quality of Service (QoS) .....	158
11.1.12.1 Type Of Service (ToS) .....	158
11.1.12.2 DiffServ .....	158
11.1.12.3 DSCP and Per-Hop Behavior .....	158
11.1.12.4 VLAN .....	159
11.2 SIP Screens .....	159
11.2.1 SIP Settings Screen.....	159
11.2.2 Advanced SIP Setup Screen .....	161
11.2.3 SIP QoS Screen .....	165
<b>Chapter 12</b>	
<b>Phone .....</b>	<b>167</b>
12.1 Phone Overview .....	167
12.1.1 Voice Activity Detection/Silence Suppression/Comfort Noise .....	167
12.1.2 Echo Cancellation .....	167
12.1.3 Supplementary Phone Services Overview .....	167
12.1.3.1 The Flash Key .....	168
12.1.3.2 Europe Type Supplementary Phone Services .....	168
12.1.3.3 USA Type Supplementary Services .....	170
12.2 Phone Screens .....	171
12.2.1 Analog Phone Screen.....	171
12.2.2 Advanced Analog Phone Setup Screen .....	172
12.2.3 Common Phone Settings Screen .....	174
12.2.4 Phone Region Screen.....	174

<b>Chapter 13</b>	
<b>Phone Book</b> .....	<b>177</b>
13.1 Phone Book Overview .....	177
13.2 Speed Dial Screen .....	177
13.3 Incoming Call Policy Screen .....	179
13.4 Group Ring Screen .....	181
<b>Chapter 14</b>	
<b>PSTN Line</b> .....	<b>185</b>
14.1 PSTN Line Overview .....	185
14.2 PSTN Line Screen .....	185
<b>Chapter 15</b>	
<b>Firewalls</b> .....	<b>187</b>
15.1 Firewall Overview .....	187
15.2 Types of Firewalls .....	187
15.2.1 Packet Filtering Firewalls .....	187
15.2.2 Application-level Firewalls .....	188
15.2.3 Stateful Inspection Firewalls .....	188
15.3 Introduction to ZyXEL's Firewall .....	188
15.3.1 Denial of Service Attacks .....	189
15.4 Denial of Service .....	189
15.4.1 Basics .....	189
15.4.2 Types of DoS Attacks .....	190
15.4.2.1 ICMP Vulnerability .....	192
15.4.2.2 Illegal Commands (NetBIOS and SMTP) .....	192
15.4.2.3 Traceroute .....	193
15.5 Stateful Inspection .....	193
15.5.1 Stateful Inspection Process .....	194
15.5.2 Stateful Inspection on Your ZyXEL Device .....	194
15.5.3 TCP Security .....	195
15.5.4 UDP/ICMP Security .....	195
15.5.5 Upper Layer Protocols .....	196
15.6 Guidelines for Enhancing Security with Your Firewall .....	196
15.6.1 Security In General .....	196
15.7 Packet Filtering Vs Firewall .....	197
15.7.1 Packet Filtering: .....	197
15.7.1.1 When To Use Filtering .....	198
15.7.2 Firewall .....	198
15.7.2.1 When To Use The Firewall .....	198

<b>Chapter 16</b>	
<b>Firewall Configuration .....</b>	<b>199</b>
16.1 Access Methods .....	199
16.2 Firewall Policies Overview .....	199
16.3 Rule Logic Overview .....	200
16.3.1 Rule Checklist .....	200
16.3.2 Security Ramifications .....	200
16.3.3 Key Fields For Configuring Rules .....	201
16.3.3.1 Action .....	201
16.3.3.2 Service .....	201
16.3.3.3 Source Address .....	201
16.3.3.4 Destination Address .....	201
16.4 Connection Direction .....	201
16.4.1 LAN to WAN Rules .....	202
16.4.2 Alerts .....	202
16.5 General Firewall Policy .....	202
16.6 Firewall Rules Summary .....	203
16.6.1 Configuring Firewall Rules .....	205
16.6.2 Customized Services .....	208
16.6.3 Configuring A Customized Service .....	209
16.7 Example Firewall Rule .....	209
16.8 DoS Thresholds .....	213
16.8.1 Threshold Values .....	213
16.8.2 Half-Open Sessions .....	214
16.8.2.1 TCP Maximum Incomplete and Blocking Time .....	214
16.8.3 Configuring Firewall Thresholds .....	215
<b>Chapter 17</b>	
<b>Content Filtering .....</b>	<b>217</b>
17.1 Content Filtering Overview .....	217
17.2 Configuring Keyword Blocking .....	217
17.3 Configuring the Schedule .....	218
17.4 Configuring Trusted Computers .....	219
<b>Chapter 18</b>	
<b>IPSec VPN .....</b>	<b>221</b>
18.1 IPSec VPN Overview .....	221
18.1.1 IKE SA Overview .....	222
18.1.1.1 IP Addresses of the ZyXEL Device and Remote IPSec Router .....	222
18.1.1.2 IKE SA Proposal .....	223
18.1.1.3 Diffie-Hellman (DH) Key Exchange .....	223
18.1.1.4 Authentication .....	224
18.1.1.5 Extended Authentication .....	225

18.1.2 Additional Topics for IKE SA .....	226
18.1.2.1 Negotiation Mode .....	226
18.1.2.2 VPN, NAT and NAT Traversal .....	226
18.1.3 IPsec SA Overview .....	227
18.1.3.1 Local Network and Remote Network .....	228
18.1.3.2 Active Protocol .....	228
18.1.3.3 Encapsulation .....	228
18.1.3.4 IPsec SA Proposal and Perfect Forward Secrecy .....	229
18.1.4 Additional Topics for IPsec SA .....	229
18.1.4.1 IPsec SA using Manual Keys .....	229
18.2 VPN Setup Screen .....	230
18.3 Editing VPN Policies .....	232
18.4 Configuring Advanced IKE Settings .....	237
18.5 Configuring Manual Key .....	240
18.6 Viewing SA Monitor .....	243
18.7 Configuring Global Setting .....	245
18.8 Telecommuter VPN/IPsec Examples .....	245
18.8.1 Telecommuters Sharing One VPN Rule Example .....	245
18.8.2 Telecommuters Using Unique VPN Rules Example .....	246
18.9 VPN and Remote Management .....	248
<b>Chapter 19</b>	
<b>Certificates.....</b>	<b>249</b>
19.1 Certificates Overview .....	249
19.1.1 Advantages of Certificates .....	250
19.2 Self-signed Certificates .....	250
19.3 Configuration Summary .....	250
19.4 My Certificates .....	251
19.5 My Certificate Import .....	253
19.5.1 Certificate File Formats .....	253
19.6 My Certificate Create .....	254
19.7 My Certificate Details .....	256
19.8 Trusted CAs .....	259
19.9 Trusted CA Import .....	261
19.10 Trusted CA Details .....	262
19.11 Trusted Remote Hosts .....	264
19.12 Verifying a Trusted Remote Host's Certificate .....	266
19.12.1 Trusted Remote Host Certificate Fingerprints .....	266
19.13 Trusted Remote Hosts Import .....	267
19.14 Trusted Remote Host Certificate Details .....	267
19.15 Directory Servers .....	270
19.16 Directory Server Add or Edit .....	271

<b>Chapter 20</b>	
<b>Static Route</b>	<b>273</b>
20.1 Static Route	273
20.2 Configuring Static Route	273
20.2.1 Static Route Edit	274
<b>Chapter 21</b>	
<b>Bandwidth Management</b>	<b>277</b>
21.1 Bandwidth Management Overview	277
21.2 Application-based Bandwidth Management	277
21.3 Subnet-based Bandwidth Management	277
21.4 Application and Subnet-based Bandwidth Management	278
21.5 Scheduler	278
21.5.1 Priority-based Scheduler	278
21.5.2 Fairness-based Scheduler	279
21.6 Maximize Bandwidth Usage	279
21.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic	279
21.6.2 Maximize Bandwidth Usage Example	280
21.6.2.1 Priority-based Allotment of Unused & Unbudgeted Bandwidth	280
21.6.2.2 Fairness-based Allotment of Unused & Unbudgeted Bandwidth	281
21.6.3 Bandwidth Management Priorities	281
21.7 Over Allotment of Bandwidth	282
21.8 Configuring Summary	282
21.9 Bandwidth Management Rule Setup	283
21.9.1 Rule Configuration	285
21.10 Bandwidth Monitor	287
<b>Chapter 22</b>	
<b>Dynamic DNS Setup</b>	<b>289</b>
22.1 Dynamic DNS Overview	289
22.1.1 DYNDNS Wildcard	289
22.2 Configuring Dynamic DNS	289
<b>Chapter 23</b>	
<b>Remote Management Configuration</b>	<b>293</b>
23.1 Remote Management Overview	293
23.1.1 Remote Management Limitations	293
23.1.2 Remote Management and NAT	294
23.1.3 System Timeout	294
23.2 Introduction to HTTPS	294
23.3 WWW	295
23.4 Telnet	296
23.5 Configuring Telnet	297

23.6 Configuring FTP .....	298
23.7 SNMP .....	299
23.7.1 Supported MIBs .....	300
23.7.2 SNMP Traps .....	300
23.7.3 Configuring SNMP .....	300
23.8 Configuring DNS .....	302
23.9 Configuring ICMP .....	302
23.10 TR-069 .....	304
<b>Chapter 24</b>	
<b>Universal Plug-and-Play (UPnP) .....</b>	<b>307</b>
24.1 Introducing Universal Plug and Play .....	307
24.1.1 How do I know if I'm using UPnP? .....	307
24.1.2 NAT Traversal .....	307
24.1.3 Cautions with UPnP .....	308
24.2 UPnP and ZyXEL .....	308
24.2.1 Configuring UPnP .....	308
24.3 Installing UPnP in Windows Example .....	309
24.4 Using UPnP in Windows XP Example .....	312
<b>Chapter 25</b>	
<b>System .....</b>	<b>319</b>
25.1 General Setup and System Name .....	319
25.1.1 General Setup .....	319
25.2 Time Setting .....	321
<b>Chapter 26</b>	
<b>Logs.....</b>	<b>325</b>
26.1 Logs Overview .....	325
26.1.1 Alerts and Logs .....	325
26.2 Viewing the Logs .....	325
26.3 Configuring Log Settings .....	326
26.4 SMTP Error Messages .....	329
26.4.1 Example E-mail Log .....	329
<b>Chapter 27</b>	
<b>Tools.....</b>	<b>331</b>
27.1 Introduction .....	331
27.2 Filename Conventions .....	331
27.3 File Maintenance Over WAN .....	332
27.4 Firmware Upgrade Screen .....	332
27.5 Backup and Restore .....	334
27.5.1 Backup Configuration .....	335



27.5.2 Restore Configuration .....	335
27.5.3 Reset to Factory Defaults .....	336
27.6 Restart .....	337
27.7 Using FTP or TFTP to Back Up Configuration .....	337
27.7.1 Using the FTP Commands to Back Up Configuration .....	337
27.7.2 FTP Command Configuration Backup Example .....	338
27.7.3 Configuration Backup Using GUI-based FTP Clients .....	338
27.7.4 Backup Configuration Using TFTP .....	339
27.7.5 TFTP Command Configuration Backup Example .....	339
27.7.6 Configuration Backup Using GUI-based TFTP Clients .....	340
27.8 Using FTP or TFTP to Restore Configuration .....	340
27.8.1 Restore Using FTP Session Example .....	341
27.9 FTP and TFTP Firmware and Configuration File Uploads .....	341
27.9.1 FTP File Upload Command from the DOS Prompt Example .....	341
27.9.2 FTP Session Example of Firmware File Upload .....	342
27.9.3 TFTP File Upload .....	342
27.9.4 TFTP Upload Command Example .....	343
<b>Chapter 28</b>	
<b>Diagnostic .....</b>	<b>345</b>
28.1 General Diagnostic .....	345
28.2 DSL Line Diagnostic .....	345
<b>Chapter 29</b>	
<b>Troubleshooting .....</b>	<b>349</b>
29.1 Problems Starting Up the ZyXEL Device .....	349
29.2 Problems with the LAN .....	349
29.3 Problems with the WAN .....	350
29.4 Problems Accessing the ZyXEL Device .....	351
29.4.1 Pop-up Windows, JavaScripts and Java Permissions .....	351
29.4.1.1 Internet Explorer Pop-up Blockers .....	352
29.4.1.2 JavaScripts .....	355
29.4.1.3 Java Permissions .....	357
29.5 Telephone Problems .....	359
<b>Appendix A</b>	
<b>Product Specifications .....</b>	<b>361</b>
Specification Tables.....	361
<b>Firmware Specifications .....</b>	<b>361</b>
P-2608HW/HWL-Dx Series Power Adaptor Specifications .....	366
<b>Appendix B</b>	
<b>Setting up Your Computer's IP Address.....</b>	<b>367</b>

Windows 95/98/Me.....	367
Configuring .....	369
Verifying Settings.....	370
Windows 2000/NT/XP .....	370
Verifying Settings.....	374
Macintosh OS 8/9.....	374
Verifying Settings.....	376
Macintosh OS X .....	376
Verifying Settings.....	377
<b>Appendix C</b>	
<b>IP Addresses and Subnetting .....</b>	<b>379</b>
Introduction to IP Addresses .....	379
IP Address Classes and Hosts .....	379
Subnet Masks .....	381
Subnetting .....	381
Example: Two Subnets .....	382
Example: Four Subnets.....	383
Example Eight Subnets.....	384
Subnetting With Class A and Class B Networks .....	385
<b>Appendix D</b>	
<b>Common Services .....</b>	<b>387</b>
<b>Appendix E</b>	
<b>Importing Certificates .....</b>	<b>389</b>
Import Prestige Certificates into Netscape Navigator .....	389
Importing the Prestige's Certificate into Internet Explorer .....	389
Enrolling and Importing SSL Client Certificates .....	393
Installing the CA's Certificate .....	394
Installing Your Personal Certificate(s).....	395
Using a Certificate When Accessing the Prestige Example.....	397
<b>Appendix F</b>	
<b>Triangle Route .....</b>	<b>399</b>
The Ideal Setup.....	399
The "Triangle Route" Problem.....	399
The "Triangle Route" Solutions .....	400
IP Aliasing .....	400
Gateways on the WAN Side.....	401
<b>Appendix G</b>	
<b>Log Descriptions.....</b>	<b>403</b>

---

Log Commands .....	412
Configuring What You Want the ZyXEL Device to Log .....	412
Displaying Logs .....	413
Log Command Example.....	414
<b>Appendix H</b>	
<b>Internal SPTGEN .....</b>	<b>415</b>
Internal SPTGEN Overview .....	415
The Configuration Text File Format.....	415
Internal SPTGEN File Modification - Important Points to Remember .....	415
Internal SPTGEN FTP Download Example.....	416
Internal SPTGEN FTP Upload Example .....	417
Command Examples .....	438
<b>Index.....</b>	<b>441</b>



# List of Figures

Figure 1 ZyXEL Device's VoIP Features .....	41
Figure 2 Internet Access .....	42
Figure 3 LEDs .....	42
Figure 4 Password Screen .....	46
Figure 5 Change Password Screen .....	46
Figure 6 Factory Default Certificate .....	47
Figure 7 Wizard or Advanced Screen .....	47
Figure 8 Main Screen .....	48
Figure 9 Select a Mode .....	53
Figure 10 Wizard Welcome .....	54
Figure 11 Auto Detection: No DSL Connection .....	54
Figure 12 Auto-Detection: PPPoE .....	55
Figure 13 Auto Detection: Failed .....	55
Figure 14 Internet Access Wizard Setup: ISP Parameters .....	56
Figure 15 Internet Connection with PPPoE .....	57
Figure 16 Internet Connection with RFC 1483 .....	57
Figure 17 Internet Connection with ENET ENCAP .....	58
Figure 18 Internet Connection with PPPoA .....	59
Figure 19 Connection Test Failed-1 .....	60
Figure 20 Connection Test Failed-2. ....	60
Figure 21 Connection Test Successful .....	61
Figure 22 Wireless LAN Setup Wizard 1 .....	61
Figure 23 Wireless LAN .....	62
Figure 24 Manually Assign a WPA key .....	63
Figure 25 Manually Assign a WEP key .....	64
Figure 26 Wireless LAN Setup 3 .....	65
Figure 27 Internet Access and WLAN Wizard Setup Complete .....	65
Figure 28 VoIP Phone Calls .....	67
Figure 29 Select a Mode .....	68
Figure 30 Wizard: Welcome .....	68
Figure 31 VoIP Wizard Configuration .....	69
Figure 32 SIP Registration Test .....	70
Figure 33 VoIP Wizard Fail .....	71
Figure 34 VoIP Wizard Finish .....	71
Figure 35 Select a Mode .....	74
Figure 36 Wizard: Welcome .....	75
Figure 37 Bandwidth Management Wizard: General Information .....	75
Figure 38 Bandwidth Management Wizard: Service Configuration .....	76

Figure 39 Bandwidth Management Wizard: Complete .....	77
Figure 40 Status Screen .....	79
Figure 41 Any IP Table .....	82
Figure 42 WLAN Status .....	83
Figure 43 Packet Statistics .....	84
Figure 44 VoIP Statistics .....	85
Figure 45 Example of Traffic Shaping .....	93
Figure 46 Internet Access Setup (PPPoE) .....	95
Figure 47 Advanced Internet Access Setup .....	97
Figure 48 WAN More Connections .....	99
Figure 49 WAN More Connections > Modify .....	100
Figure 50 Traffic Redirect Example .....	102
Figure 51 Traffic Redirect LAN Setup .....	103
Figure 52 LAN and WAN IP Addresses .....	105
Figure 53 Any IP Example .....	110
Figure 54 LAN IP .....	111
Figure 55 Advanced LAN Setup .....	112
Figure 56 DHCP Setup .....	113
Figure 57 LAN Client List .....	114
Figure 58 Physical Network & Partitioned Logical Networks .....	116
Figure 59 LAN IP Alias .....	116
Figure 60 Example of a Wireless Network .....	119
Figure 61 Wireless LAN: General .....	123
Figure 62 Wireless: No Security .....	125
Figure 63 Wireless: Static WEP Encryption .....	126
Figure 64 Wireless: WPA(2)-PSK .....	127
Figure 65 Wireless: WPA(2) .....	128
Figure 66 Advanced .....	130
Figure 67 Network > Wireless LAN > OTIST .....	131
Figure 68 Example: Wireless Client OTIST Screen .....	132
Figure 69 OTIST: Settings .....	132
Figure 70 OTIST In Progress Screen on the ZyXEL Device .....	132
Figure 71 OTIST: In Progress on the Wireless Device .....	133
Figure 72 Start OTIST? .....	133
Figure 73 MAC Address Filter .....	134
Figure 74 Application Priority Configuration .....	136
Figure 75 How NAT Works .....	140
Figure 76 NAT Application With IP Alias .....	141
Figure 77 NAT General .....	143
Figure 78 Multiple Servers Behind NAT Example .....	144
Figure 79 Port Forwarding .....	145
Figure 80 Port Forwarding Rule Setup .....	146
Figure 81 Address Mapping Rules .....	147

Figure 82 Edit Address Mapping Rule .....	148
Figure 83 Network > NAT > ALG .....	150
Figure 84 SIP User Agent .....	153
Figure 85 SIP Proxy Server .....	153
Figure 86 SIP Redirect Server .....	154
Figure 87 STUN .....	156
Figure 88 DiffServ: Differentiated Service Field .....	158
Figure 89 VoIP > SIP > SIP Settings .....	160
Figure 90 VoIP > SIP > SIP Settings > Advanced .....	162
Figure 91 VoIP > SIP > QoS .....	165
Figure 92 VoIP > Phone > Analog Phone .....	172
Figure 93 VoIP > Phone > Analog Phone > Advanced .....	173
Figure 94 VoIP > Phone > Common .....	174
Figure 95 VoIP > Phone > Region .....	175
Figure 96 Phone Book > Speed Dial .....	178
Figure 97 Phone Book > Incoming Call Policy .....	180
Figure 98 Phone Book > Group Ring .....	182
Figure 99 VoIP > PSTN Line > General .....	186
Figure 100 Firewall Application .....	189
Figure 101 Three-Way Handshake .....	190
Figure 102 SYN Flood .....	191
Figure 103 Smurf Attack .....	192
Figure 104 Stateful Inspection .....	193
Figure 105 Firewall: General .....	202
Figure 106 Firewall Rules .....	204
Figure 107 Firewall: Edit Rule .....	206
Figure 108 Firewall: Customized Services .....	208
Figure 109 Firewall: Configure Customized Services .....	209
Figure 110 Firewall Example: Rules .....	210
Figure 111 Edit Custom Port Example .....	210
Figure 112 Firewall Example: Edit Rule: Destination Address .....	211
Figure 113 Firewall Example: Edit Rule: Select Customized Services .....	212
Figure 114 Firewall Example: Rules: MyService .....	213
Figure 115 Firewall: Threshold .....	215
Figure 116 Content Filter: Keyword .....	217
Figure 117 Content Filter: Schedule .....	218
Figure 118 Content Filter: Trusted .....	219
Figure 119 VPN: Example .....	221
Figure 120 VPN: IKE SA and IPSec SA .....	222
Figure 121 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal .....	223
Figure 122 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange .....	223
Figure 123 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication .....	224
Figure 124 VPN/NAT Example .....	227

Figure 125 VPN: Transport and Tunnel Mode Encapsulation .....	228
Figure 126 VPN Setup .....	231
Figure 127 Edit VPN Policies .....	233
Figure 128 Advanced VPN Policies .....	238
Figure 129 VPN: Manual Key .....	241
Figure 130 VPN: SA Monitor .....	244
Figure 131 VPN: Global Setting .....	245
Figure 132 Telecommuters Sharing One VPN Rule Example .....	246
Figure 133 Telecommuters Using Unique VPN Rules Example .....	247
Figure 134 Certificate Configuration Overview .....	250
Figure 135 My Certificates .....	251
Figure 136 My Certificate Import .....	253
Figure 137 My Certificate Create .....	254
Figure 138 My Certificate Details .....	257
Figure 139 Trusted CAs .....	260
Figure 140 Trusted CA Import .....	261
Figure 141 Trusted CA Details .....	262
Figure 142 Trusted Remote Hosts .....	265
Figure 143 Remote Host Certificates .....	266
Figure 144 Certificate Details .....	266
Figure 145 Trusted Remote Host Import .....	267
Figure 146 Trusted Remote Host Details .....	268
Figure 147 Directory Servers .....	271
Figure 148 Directory Server Add .....	272
Figure 149 Example of Static Routing Topology .....	273
Figure 150 Static Route .....	274
Figure 151 Static Route Edit .....	275
Figure 152 Subnet-based Bandwidth Management Example .....	278
Figure 153 Bandwidth Management: Summary .....	282
Figure 154 Bandwidth Management: Rule Setup .....	284
Figure 155 Bandwidth Management Rule Configuration .....	285
Figure 156 Bandwidth Management: Monitor .....	287
Figure 157 Dynamic DNS .....	290
Figure 158 HTTPS Implementation .....	295
Figure 159 Remote Management: WWW .....	295
Figure 160 Telnet Configuration on a TCP/IP Network .....	297
Figure 161 Remote Management: Telnet .....	297
Figure 162 Remote Management: FTP .....	298
Figure 163 SNMP Management Model .....	299
Figure 164 Remote Management: SNMP .....	301
Figure 165 Remote Management: DNS .....	302
Figure 166 Remote Management: ICMP .....	303
Figure 167 Enabling TR-069 .....	304



Figure 168 Configuring UPnP .....	308
Figure 169 Add/Remove Programs: Windows Setup: Communication .....	310
Figure 170 Add/Remove Programs: Windows Setup: Communication: Components 310	
Figure 171 Network Connections .....	311
Figure 172 Windows Optional Networking Components Wizard .....	311
Figure 173 Networking Services .....	312
Figure 174 Network Connections .....	313
Figure 175 Internet Connection Properties .....	313
Figure 176 Internet Connection Properties: Advanced Settings .....	314
Figure 177 Internet Connection Properties: Advanced Settings: Add .....	314
Figure 178 System Tray Icon .....	315
Figure 179 Internet Connection Status .....	315
Figure 180 Network Connections .....	316
Figure 181 Network Connections: My Network Places .....	317
Figure 182 Network Connections: My Network Places: Properties: Example .....	317
Figure 183 System General Setup .....	320
Figure 184 System Time Setting .....	321
Figure 185 View Log .....	326
Figure 186 Log Settings .....	327
Figure 187 E-mail Log Example .....	330
Figure 188 Firmware Upgrade .....	333
Figure 189 Firmware Upload In Progress .....	333
Figure 190 Network Temporarily Disconnected .....	334
Figure 191 Error Message .....	334
Figure 192 Configuration .....	335
Figure 193 Configuration Upload Successful .....	336
Figure 194 Network Temporarily Disconnected .....	336
Figure 195 Reset Warning Message .....	336
Figure 196 Reset In Process Message .....	337
Figure 197 Restart Screen .....	337
Figure 198 FTP Session Example .....	338
Figure 199 Restore Using FTP Session Example .....	341
Figure 200 FTP Session Example of Firmware File Upload .....	342
Figure 201 Diagnostic: General .....	345
Figure 202 Diagnostic: DSL Line .....	346
Figure 203 Pop-up Blocker .....	352
Figure 204 Internet Options .....	353
Figure 205 Internet Options .....	354
Figure 206 Pop-up Blocker Settings .....	355
Figure 207 Internet Options .....	356
Figure 208 Security Settings - Java Scripting .....	357
Figure 209 Security Settings - Java .....	358

Figure 210 Java (Sun) .....	359
Figure 211 Windows 95/98/Me: Network: Configuration .....	368
Figure 212 Windows 95/98/Me: TCP/IP Properties: IP Address .....	369
Figure 213 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	370
Figure 214 Windows XP: Start Menu .....	371
Figure 215 Windows XP: Control Panel .....	371
Figure 216 Windows XP: Control Panel: Network Connections: Properties .....	372
Figure 217 Windows XP: Local Area Connection Properties .....	372
Figure 218 Windows XP: Advanced TCP/IP Settings .....	373
Figure 219 Windows XP: Internet Protocol (TCP/IP) Properties .....	374
Figure 220 Macintosh OS 8/9: Apple Menu .....	375
Figure 221 Macintosh OS 8/9: TCP/IP .....	375
Figure 222 Macintosh OS X: Apple Menu .....	376
Figure 223 Macintosh OS X: Network .....	377
Figure 224 Security Certificate .....	389
Figure 225 Login Screen .....	390
Figure 226 Certificate General Information before Import .....	390
Figure 227 Certificate Import Wizard 1 .....	391
Figure 228 Certificate Import Wizard 2 .....	391
Figure 229 Certificate Import Wizard 3 .....	392
Figure 230 Root Certificate Store .....	392
Figure 231 Certificate General Information after Import .....	393
Figure 232 Prestige Trusted CA Screen .....	394
Figure 233 CA Certificate Example .....	394
Figure 234 Personal Certificate Import Wizard 1 .....	395
Figure 235 Personal Certificate Import Wizard 2 .....	395
Figure 236 Personal Certificate Import Wizard 3 .....	396
Figure 237 Personal Certificate Import Wizard 4 .....	396
Figure 238 Personal Certificate Import Wizard 5 .....	397
Figure 239 Personal Certificate Import Wizard 6 .....	397
Figure 240 Access the Prestige Via HTTPS .....	397
Figure 241 SSL Client Authentication .....	398
Figure 242 Prestige Secure Login Screen .....	398
Figure 243 Ideal Setup .....	399
Figure 244 "Triangle Route" Problem .....	400
Figure 245 IP Alias .....	401
Figure 246 Gateways on the WAN Side .....	401
Figure 247 Displaying Log Categories Example .....	412
Figure 248 Displaying Log Parameters Example .....	413
Figure 249 Log Command Example .....	414
Figure 250 Configuration Text File Format: Column Descriptions .....	415
Figure 251 Invalid Parameter Entered: Command Line Example .....	416
Figure 252 Valid Parameter Entered: Command Line Example .....	416

Figure 253 Internal SPTGEN FTP Download Example ..... 417  
Figure 254 Internal SPTGEN FTP Upload Example ..... 417



# List of Tables

Table 1 Models Covered .....	41
Table 2 LEDs .....	43
Table 3 Web Configurator Icons in the Title Bar .....	49
Table 4 Navigation Panel Summary .....	49
Table 5 Internet Access Wizard Setup: ISP Parameters .....	56
Table 6 Internet Connection with PPPoE .....	57
Table 7 Internet Connection with RFC 1483 .....	58
Table 8 Internet Connection with ENET ENCAP .....	58
Table 9 Internet Connection with PPPoA .....	59
Table 10 Wireless LAN Setup Wizard 1 .....	61
Table 11 Wireless LAN Setup Wizard 2 .....	62
Table 12 Manually Assign a WPA key .....	63
Table 13 Manually Assign a WEP key .....	64
Table 14 Sample SIP Account Information .....	69
Table 15 VoIP Wizard Configuration .....	69
Table 16 Media Bandwidth Management Setup: Services .....	73
Table 17 Bandwidth Management Wizard: General Information .....	75
Table 18 Bandwidth Management Wizard: Service Configuration .....	76
Table 19 Status Screen .....	80
Table 20 Any IP Table .....	83
Table 21 WLAN Status .....	83
Table 22 Packet Statistics .....	84
Table 23 VoIP Statistics .....	86
Table 24 Internet Access Setup .....	95
Table 25 Advanced Internet Access Setup .....	97
Table 26 WAN More Connections .....	99
Table 27 WAN More Connections > Modify .....	100
Table 28 WAN Backup Setup .....	104
Table 29 LAN IP .....	111
Table 30 Advanced LAN Setup .....	112
Table 31 DHCP Setup .....	113
Table 32 LAN Client List .....	115
Table 33 LAN IP Alias .....	116
Table 34 Types of Encryption for Each Type of Authentication .....	121
Table 35 Wireless LAN: General .....	124
Table 36 Wireless No Security .....	125
Table 37 Wireless: Static WEP Encryption .....	126
Table 38 Wireless: WPA(2)-PSK .....	127

Table 39 Wireless: WPA(2)	128
Table 40 Wireless LAN: Advanced	130
Table 41 Network > Wireless LAN > OTIST	131
Table 42 MAC Address Filter	134
Table 43 Wireless LAN: QoS	135
Table 44 Application Priority Configuration	136
Table 45 NAT Definitions	139
Table 46 NAT Mapping Types	142
Table 47 NAT General	143
Table 48 Port Forwarding	145
Table 49 Port Forwarding Rule Setup	146
Table 50 Address Mapping Rules	147
Table 51 Edit Address Mapping Rule	149
Table 52 Network > NAT > ALG	150
Table 53 SIP Call Progression	152
Table 54 Custom Tones Details	157
Table 55 VoIP > SIP > SIP Settings	160
Table 56 VoIP > SIP Settings > Advanced	162
Table 57 VoIP > SIP > QoS	165
Table 58 European Type Flash Key Commands	168
Table 59 USA Type Flash Key Commands	170
Table 60 VoIP > Phone > Analog Phone	172
Table 61 VoIP > Phone > Analog Phone > Advanced	173
Table 62 VoIP > Phone > Common	174
Table 63 VoIP > Phone > Region	175
Table 64 Phone Book > Speed Dial	178
Table 65 Phone Book > Incoming Call Policy	180
Table 66 Phone Book > Group Ring	182
Table 67 VoIP > PSTN Line > General	186
Table 68 Common IP Ports	190
Table 69 ICMP Commands That Trigger Alerts	192
Table 70 Legal NetBIOS Commands	192
Table 71 Legal SMTP Commands	192
Table 72 Firewall: General	203
Table 73 Firewall Rules	204
Table 74 Firewall: Edit Rule	207
Table 75 Customized Services	208
Table 76 Firewall: Configure Customized Services	209
Table 77 Firewall: Threshold	215
Table 78 Content Filter: Keyword	218
Table 79 Content Filter: Schedule	219
Table 80 Content Filter: Trusted	219
Table 81 VPN Example: Matching ID Type and Content	224

Table 82 VPN Example: Mismatching ID Type and Content .....	225
Table 83 VPN Setup .....	231
Table 84 Edit VPN Policies .....	233
Table 85 Advanced VPN Policies .....	238
Table 86 VPN: Manual Key .....	241
Table 87 VPN: SA Monitor .....	244
Table 88 VPN: Global Setting .....	245
Table 89 Telecommuters Sharing One VPN Rule Example .....	246
Table 90 Telecommuters Using Unique VPN Rules Example .....	247
Table 91 My Certificates .....	251
Table 92 My Certificate Import .....	254
Table 93 My Certificate Create .....	255
Table 94 My Certificate Details .....	258
Table 95 Trusted CAs .....	260
Table 96 Trusted CA Import .....	261
Table 97 Trusted CA Details .....	263
Table 98 Trusted Remote Hosts .....	265
Table 99 Trusted Remote Host Import .....	267
Table 100 Trusted Remote Host Details .....	269
Table 101 Directory Servers .....	271
Table 102 Directory Server Add .....	272
Table 103 Static Route .....	274
Table 104 Static Route Edit .....	275
Table 105 Application and Subnet-based Bandwidth Management Example .....	278
Table 106 Maximize Bandwidth Usage Example .....	280
Table 107 Priority-based Allotment of Unused & Unbudgeted Bandwidth Example 280	
Table 108 Fairness-based Allotment of Unused & Unbudgeted Bandwidth Example 281	
Table 109 Bandwidth Management Priorities .....	281
Table 110 Over Allotment of Bandwidth Example .....	282
Table 111 Media Bandwidth Management: Summary .....	283
Table 112 Bandwidth Management: Rule Setup .....	284
Table 113 Bandwidth Management Rule Configuration .....	285
Table 114 Dynamic DNS .....	290
Table 115 Remote Management: WWW .....	296
Table 116 Remote Management: Telnet .....	297
Table 117 Remote Management: FTP .....	298
Table 118 SNMP Traps .....	300
Table 119 Remote Management: SNMP .....	301
Table 120 Remote Management: DNS .....	302
Table 121 Remote Management: ICMP .....	303
Table 122 TR-069 Commands .....	304

Table 123 Configuring UPnP .....	309
Table 124 System General Setup .....	320
Table 125 System Time Setting .....	321
Table 126 View Log .....	326
Table 127 Log Settings .....	327
Table 128 SMTP Error Messages .....	329
Table 129 Filename Conventions .....	332
Table 130 Firmware Upgrade .....	333
Table 131 Restore Configuration .....	335
Table 132 General Commands for GUI-based FTP Clients .....	338
Table 133 General Commands for GUI-based TFTP Clients .....	340
Table 134 Diagnostic: General .....	345
Table 135 Diagnostic: DSL Line .....	346
Table 136 Troubleshooting Starting Up Your Device .....	349
Table 137 Troubleshooting the LAN .....	349
Table 138 Troubleshooting the WAN .....	350
Table 139 Troubleshooting Accessing Your Device .....	351
Table 140 Troubleshooting Telephone .....	359
Table 141 Device Specifications .....	361
Table 142 Firmware Features .....	361
Table 143 Firmware Specifications .....	364
Table 144 P-2608HW/HWL-Dx Series Power Adaptor Specifications .....	366
Table 145 Classes of IP Addresses .....	380
Table 146 Allowed IP Address Range By Class .....	380
Table 147 "Natural" Masks .....	381
Table 148 Alternative Subnet Mask Notation .....	381
Table 149 Two Subnets Example .....	382
Table 150 Subnet 1 .....	382
Table 151 Subnet 2 .....	383
Table 152 Subnet 1 .....	383
Table 153 Subnet 2 .....	384
Table 154 Subnet 3 .....	384
Table 155 Subnet 4 .....	384
Table 156 Eight Subnets .....	385
Table 157 Class C Subnet Planning .....	385
Table 158 Class B Subnet Planning .....	386
Table 159 Commonly Used Services .....	387
Table 160 System Maintenance Logs .....	403
Table 161 System Error Logs .....	404
Table 162 Access Control Logs .....	404
Table 163 TCP Reset Logs .....	405
Table 164 Packet Filter Logs .....	405
Table 165 ICMP Logs .....	405



Table 166 CDR Logs .....	406
Table 167 PPP Logs .....	406
Table 168 UPnP Logs .....	407
Table 169 Content Filtering Logs .....	407
Table 170 Attack Logs .....	407
Table 171 802.1X Logs .....	408
Table 172 ACL Setting Notes .....	409
Table 173 ICMP Notes .....	409
Table 174 Syslog Logs .....	410
Table 175 SIP Logs .....	410
Table 176 RTP Logs .....	411
Table 177 FSM Logs: Caller Side .....	411
Table 178 FSM Logs: Callee Side .....	411
Table 179 Lifeline Logs .....	411
Table 180 RFC-2408 ISAKMP Payload Types .....	412
Table 181 Abbreviations Used in the Example Internal SPTGEN Screens Table ..	417
Table 182 Menu 1 General Setup .....	418
Table 183 Menu 3 .....	418
Table 184 Menu 4 Internet Access Setup .....	421
Table 185 Menu 12 .....	423
Table 186 Menu 15 SUA Server Setup .....	427
Table 187 Menu 21.1 Filter Set #1 .....	429
Table 188 Menu 21.1 Filter Set #2, .....	432
Table 189 Menu 23 System Menus .....	437
Table 190 Menu 24.11 Remote Management Control .....	438
Table 191 Command Examples .....	438



# Preface

Congratulations on your purchase of the P-2608HWL-Dx ADSL VoIP IAD with 802.11g Wireless (the “ZyXEL Device”).

Your ZyXEL Device is easy to install and configure.

## About This User's Guide

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

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

## Related Documentation

- Supporting Disk

Refer to the included CD for support documents.

- Quick Start Guide

The Quick Start Guide is designed to help you get up and running right away. It contains connection information and instructions on getting started.

- ZyXEL Web Site

Please go to <http://www.zyxel.com> for product news, firmware, updated documents, and other support materials.

## User Guide Feedback










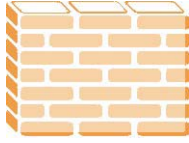

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw) or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu,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

## Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choices.
- Screen titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a right angle bracket ( > ). For example, “In Windows, click **Start** > **Settings** > **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

- The P-2608HWL-Dx series may be referred to as the "ZyXEL Device" or the "device" in this user's guide. This refers to all models (ADSL over POTS, ADSL over ISDN and ADSL over T-ISDN) unless specifically identified.

### Graphics Icons Key

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

# CHAPTER 1

## Getting To Know the ZyXEL Device

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

### 1.1 Overview

The P-2608HWL-Dx series are Integrated Access Devices (IADs) that combine an ADSL2+ router with Voice over IP (VoIP) communication capabilities. This guide covers the following models.

**Table 1** Models Covered

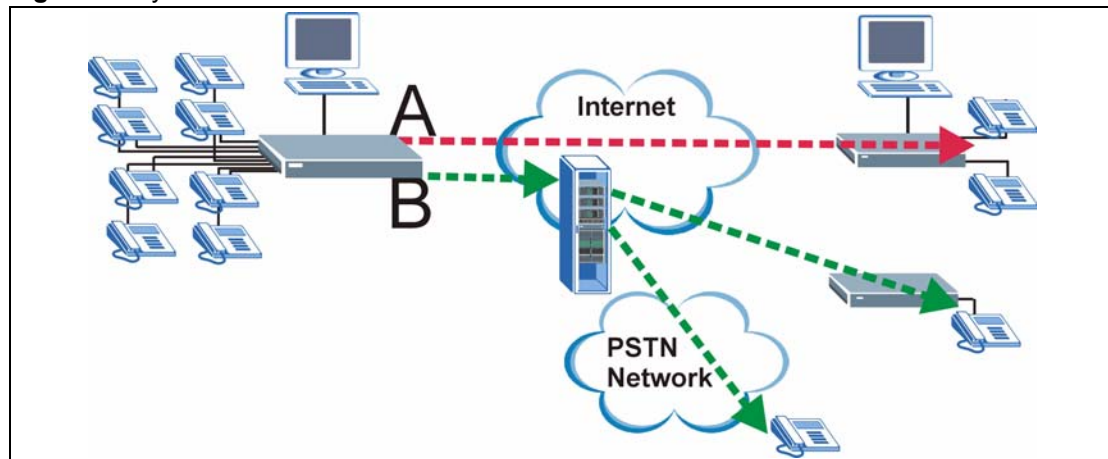
P-2608HWL-D1	P-2608HWL-D3	P-2608HWL-D7
--------------	--------------	--------------

See [Appendix A on page 361](#) for a complete list of software features.

#### 1.1.1 VoIP Features

You can use the ZyXEL Device to make and receive VoIP telephone calls:

**Figure 1** ZyXEL Device's VoIP Features

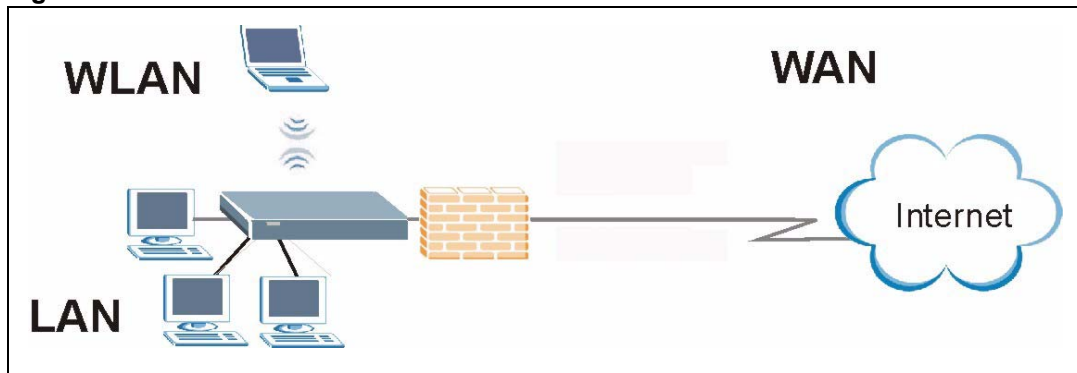


- Peer-to-Peer calls (A) - Use the ZyXEL Device to make a call to the recipient's IP address without using a SIP proxy server.
- Calls via a VoIP service provider (B) - The ZyXEL Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

## 1.1.2 DSL Router

Your ZyXEL Device is an ideal solution for fast Internet access. Computers can connect to the ZyXEL Device's LAN ports (or wirelessly) and use it as a gateway to the Internet.

**Figure 2** Internet Access



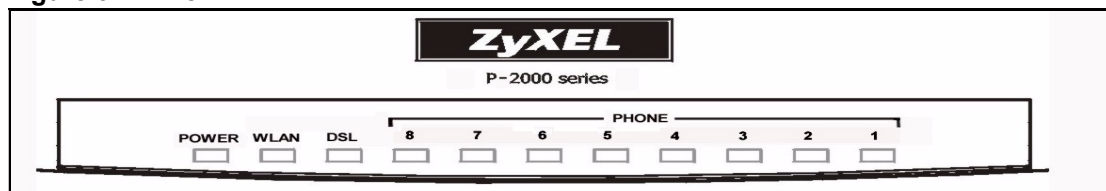
You can also configure firewall and content filtering on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed,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

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

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

## 1.2 LEDs (Lights)

**Figure 3** LEDs



The following table describes your device's LEDs.

**Table 2** LEDs

LIGHT	COLOR	STATUS	DESCRIPTION
<b>POWER</b>	Green	On	Your device is receiving power and functioning properly.
		Blinking	Your device is rebooting and performing a self-test.
	Red	On	Your device is not receiving enough power.
	None	Off	Your device is not ready or has malfunctioned.
<b>WLAN</b>	Green	On	Your device is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	Your device is sending/receiving data through the wireless LAN.
	None	Off	The wireless LAN is not ready or has failed.
<b>DSL</b>	Green	On	Your device has a DSL connection.
		Blinking	Your device is initializing the DSL line.
	None	Off	The DSL link is down.
<b>PHONE 1-8</b>	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
	None	Off	The phone port does not have a SIP account registered.





# CHAPTER 2

## Introducing the Web Configurator

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

### 2.1 Web Configurator Overview

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

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

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

See [Chapter 29 on page 349](#) if you need to make sure these functions are allowed in Internet Explorer.

#### 2.1.1 Accessing the Web Configurator

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

**Figure 4** Password Screen

The screenshot shows the ZyXEL login screen for the P-2608HWL-D1 router. At the top is the ZyXEL logo. Below it, the model number 'P-2608HWL-D1' is displayed. The text reads: 'Welcome to your router Configuration Interface' and 'Enter your password and press enter or click "Login"'. There is a password input field with a key icon and the text 'Password: \*\*\*\*'. Below the field are two buttons: 'Login' and 'Cancel'.

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

**Figure 5** Change Password Screen

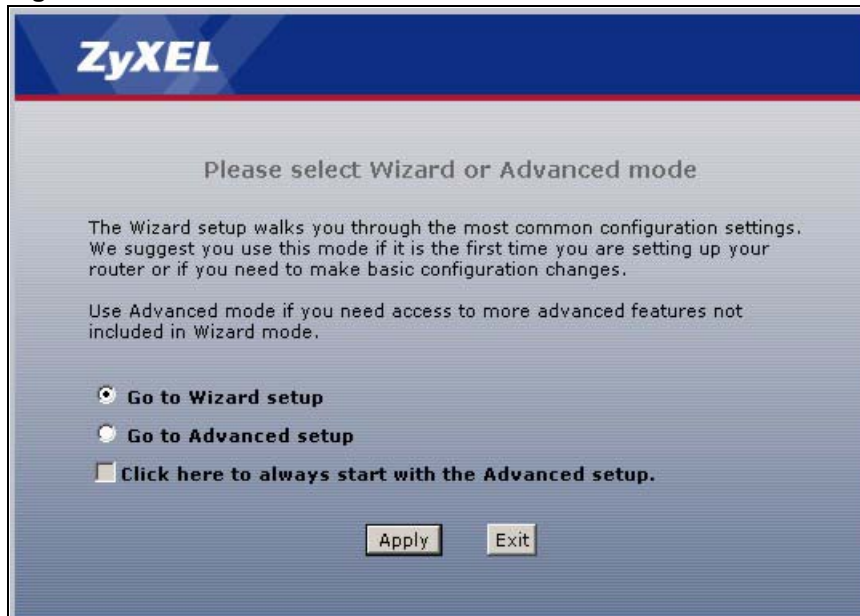
The screenshot shows the ZyXEL change password screen. At the top is the ZyXEL logo. Below it, the text reads: 'Use this screen to change the password.' and 'Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this 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 is the instruction: 'Enter your new password in the two fields below and click "Apply". Otherwise click "Ignore" to keep the default password'. There are two input fields: 'New Password:' and 'Retype to Confirm:'. Below the fields are two buttons: 'Apply' and 'Ignore'.

- 6** A screen displays to let you change your default factory certificate.
- Click **Apply** if you want to create a unique certificate for your ZyXEL Device.
  - Click **Ignore** if you don't want to create a unique certificate at this time.

**Figure 6** Factory Default Certificate

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

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

**Figure 7** Wizard or Advanced Screen

## 2.1.2 The RESET Button

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

### 2.1.2.1 Using The Reset Button

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

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

You can also use the reset button to activate OTIST by pressing the **RESET** button for 5 seconds. See [Section 9.2.5 on page 122](#) for more information on OTIST.

## 2.2 Web Configurator Main Screen

Figure 8 Main Screen

The screenshot shows the ZyXEL web configurator main screen. The interface is divided into several parts, labeled A through D:

- A**: The top title bar, which includes the ZyXEL logo and a status indicator.
- B**: The left navigation menu, which includes links for Status, Network, VoIP, Security, Advanced, and Maintenance.
- C**: The main content area, which is divided into several sections:
  - Device Information**: Host Name: P2608HWL, Model Number: P-2608HWL-D1, MAC Address: 00:13:49:00:00:01, ZyNOS Firmware Version: V3.40(ADT.0)b1 | 03/24/2006, DSL Firmware Version: TI AR7 06.00.02.00.
  - System Status**: System Uptime: 0:01:08, Current Date/Time: 01/01/2000 00:01:25, System Mode: Routing / Bridging, CPU Usage: 8.29%, Memory Usage: 23%.
  - Interface Status**: A table showing the status of the DSL, LAN, and WLAN interfaces.
  - Security**: Firewall: Enabled, Content Filter: Disable.
- D**: The bottom status bar, which shows the message "Ready".

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

- **A** - title bar

- **B** - navigation panel
- **C** - main window
- **D** - status bar



## 2.2.1 Title Bar

The title bar provides some icons in the upper right corner.



The icons provide the following functions.

**Table 3** Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	<b>Wizards:</b> Click this icon to go to the configuration wizards. See <a href="#">Chapter 3 on page 53</a> for more information.
	<b>Logout:</b> Click this icon to log out of the web configurator.

## 2.2.2 Navigation Panel

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

**Table 4** Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen contains administrative and system-related information.
Network		
WAN	Internet Access Setup	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to configure additional WAN connections.
	WAN Backup Setup	Use this screen to configure a backup gateway.
LAN	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
	DHCP Setup	Use this screen to configure a DHCP server.
	Client List	Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names).
	IP Alias	Use this screen to partition your LAN interface into subnets.

**Table 4** Navigation Panel Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	OTIST	Use this screen to configure a setup key for OTIST as well as start OTIST on the ZyXEL Device.
	MAC Filter	Use this screen to configure the ZyXEL Device to give exclusive access to specific wireless clients or exclude specific wireless clients from accessing the ZyXEL Device.
	QoS	WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	ALG	Use this screen to enable SIP ALG.
VoIP		
SIP	SIP Settings	Use this screen to configure your ZyXEL Device's Voice over IP settings.
	QoS	Use this screen to configure your ZyXEL Device's Quality of Service settings for VoIP.
Phone	Analog Phone	Use this screen to set which phone ports use which SIP accounts.
	Common	Use this screen to configure general phone port settings.
	Region	Use this screen to select your location and call service mode.
Phone Book	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
	Incoming Call Policy	Use this screen to configure call-forwarding.
	Group Ring	Use this screen to configure ring tone behavior based on the origin of incoming calls.
PSTN Line ("L" models only)	General	Use this screen to configure your ZyXEL Device's settings for PSTN calls.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Threshold	Use this screen to configure the thresholds for determining when to drop sessions that do not become fully established.
Content Filter	Keyword	Use this screen to block access to web sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for your device to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering.

**Table 4** Navigation Panel Summary

LINK	TAB	FUNCTION
VPN	Setup	Use this screen to configure each VPN tunnel.
	Monitor	Use this screen to look at the current status of each VPN tunnel.
	VPN Global Setting	Use this screen to allow NetBIOS traffic through VPN tunnels.
Certificates	My Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.
	Trusted CAs	Use this screen to save CA certificates to the ZyXEL Device.
	Trusted Remote Hosts	Use this screen to import self-signed certificates.
	Directory Servers	Use this screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).
Advanced		
Static Route	Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Bandwidth MGMT	Summary	Use this screen to configure bandwidth management on an interface.
	Rule Setup	Use this screen to define a bandwidth rule.
	Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	ICMP	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
UPnP	General	Use this screen to turn UPnP on or off.
Maintenance		
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.

**Table 4** Navigation Panel Summary

LINK	TAB	FUNCTION
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
	DSL Line	These screen displays information to help you identify problems with the DSL connection.

### Main Window

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

Right after you log in, the **Status** screen is displayed. See [Chapter 6 on page 79](#) for more information about the **Status** screen.

### 2.2.3 Status Bar

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



# CHAPTER 3

## Internet and Wireless Setup Wizard


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

### 3.1 Introduction

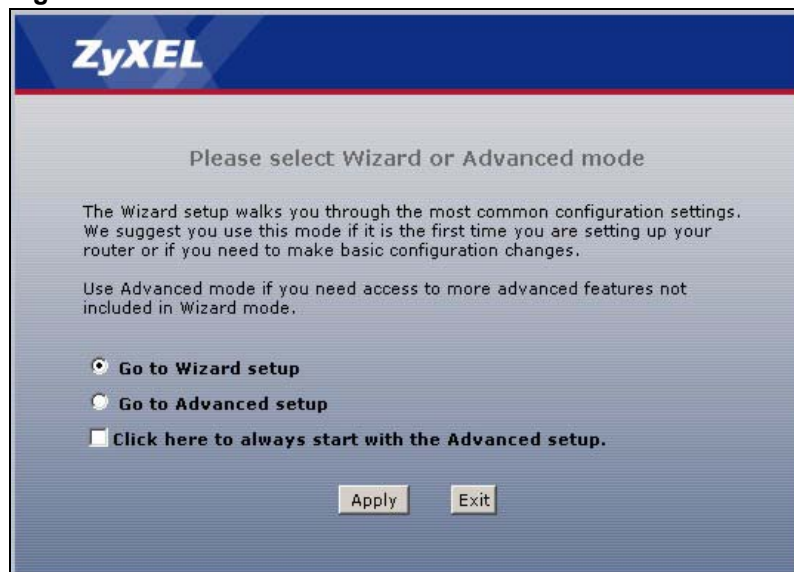
Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.

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

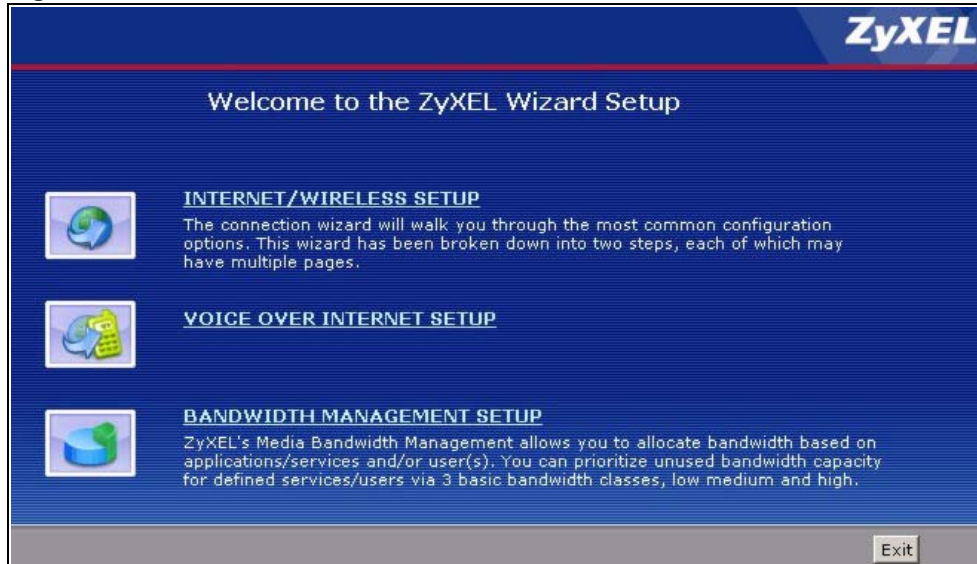
### 3.2 Internet Access Wizard Setup

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

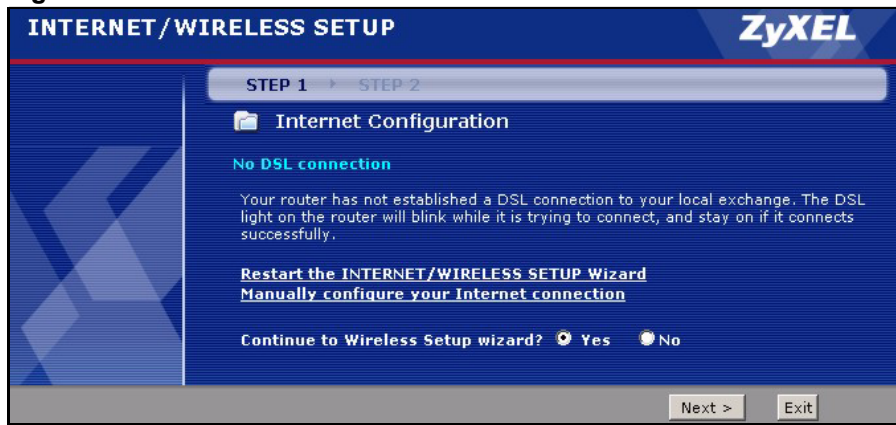
**Figure 9** Select a Mode



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

**Figure 10** Wizard Welcome

- 3 Your ZyXEL Device attempts to detect your DSL connection and your connection type.
- a The following screen appears if a connection is not detected. Check your hardware connections and click **Restart the Internet/Wireless Setup Wizard** to return to the wizard welcome screen or click **Manually configure your Internet connection** if you want to set up the connection manually. If you would like to skip your Internet setup and configure the wireless LAN settings, leave **Yes** selected and click **Next**.

**Figure 11** Auto Detection: No DSL Connection

- b The following screen displays if a PPPoE or PPPoA connection is detected. Enter your Internet account information (username, password and/or service name) exactly as provided by your ISP. Then click **Next** and see [Section 3.3 on page 60](#) for wireless connection wizard setup.

**Figure 12** Auto-Detection: PPPoE

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

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

**Figure 13** Auto Detection: Failed

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

### 3.2.1 Manual Configuration

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

**Figure 14** Internet Access Wizard Setup: ISP Parameters

**STEP 1** ▶ **STEP 2**

**Internet Configuration**

**ISP Parameters for Internet Access**

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

**Mode**  **Routing**

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

**Encapsulation**  **ENET ENCAP**

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

**Multiplexing**  **LLC**

Select the multiplexing type used by your ISP.

**Virtual Circuit ID**

**VPI**  **8**

**VCI**  **35**

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

The following table describes the fields in this screen.

**Table 5** Internet Access Wizard Setup: ISP Parameters

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

- 2 The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue. See [Section 3.3 on page 60](#) for wireless connection wizard setup

**Figure 15** Internet Connection with PPPoE

**STEP 1** ▶ **STEP 2**

**Internet Configuration**

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

User Name

Password

Service Name  (optional)

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

< Back   Apply   Exit

The following table describes the fields in this screen.

**Table 6** Internet Connection with PPPoE

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

**Figure 16** Internet Connection with RFC 1483

**STEP 1** ▶ **STEP 2**

**Internet Configuration**

**ISP Parameters for Internet Access**

IP Address

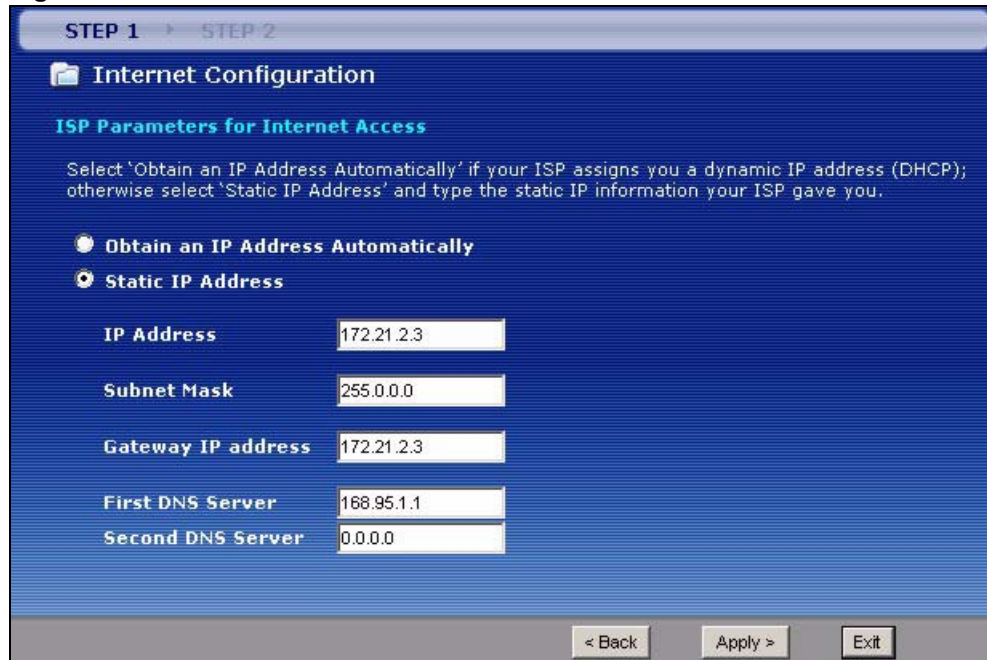
< Back   Next >   Exit

The following table describes the fields in this screen.

**Table 7** Internet Connection with RFC 1483

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

**Figure 17** Internet Connection with ENET ENCAP



The following table describes the fields in this screen.

**Table 8** Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address.
Static IP Address	Select <b>Static IP Address</b> if your ISP gave you an IP address to use.
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask If you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use <b>ENET ENCAP</b> in the <b>Encapsulation</b> field in the previous screen.



**Table 8** Internet Connection with ENET ENCAP (continued)

LABEL	DESCRIPTION
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click <b>Back</b> to go back to the previous wizard screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

**Figure 18** Internet Connection with PPPoA

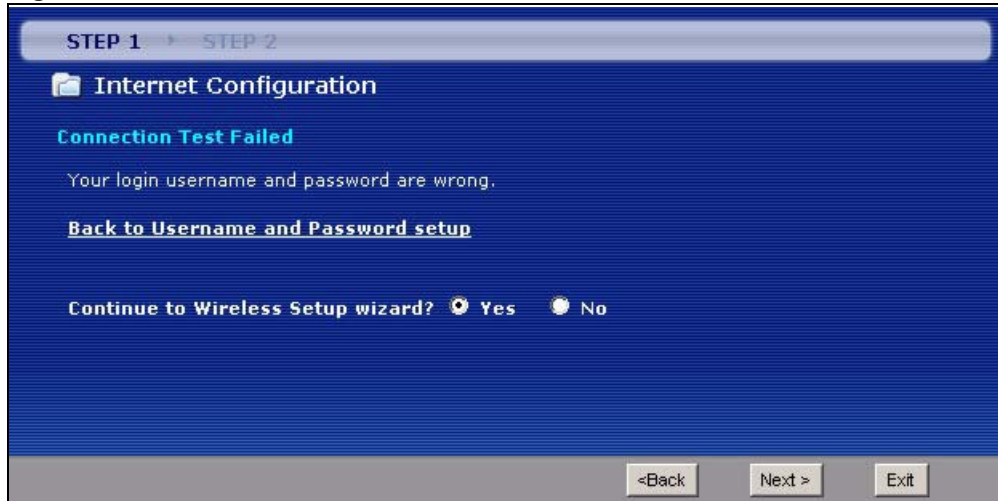
The screenshot shows a blue-themed wizard interface. At the top, it says 'STEP 1' and 'STEP 2'. Below that is a folder icon and the text 'Internet Configuration'. Underneath is the heading 'ISP Parameters for Internet Access' followed by the instruction 'Please enter the User Name and Password given to you by your Internet Service Provider here'. There are two input fields: 'User Name' and 'Password'. A yellow note icon is followed by the text: 'Note: Device is automatically configured to obtain an IP address automatically. The ISP will assign you a different one each time you connect to the Internet.' At the bottom right, there are three buttons: '< Back', 'Apply', and 'Exit'.

The following table describes the fields in this screen.

**Table 9** Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Back	Click <b>Back</b> to go back to the previous wizard screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

- If the user name and/or password you entered for PPPoE or PPPoA connection are not correct, the screen displays as shown next. Click **Back to Username and Password setup** to go back to the screen where you can modify them.

**Figure 19** Connection Test Failed-1

- If the following screen displays, check if your account is activated or click **Restart the Internet/Wireless Setup Wizard** to verify your Internet access settings.

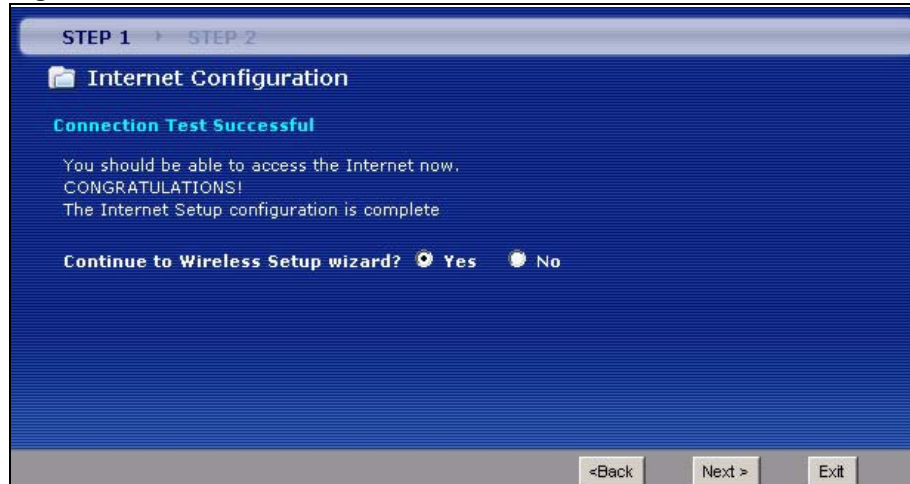
**Figure 20** Connection Test Failed-2.

### 3.3 Wireless Connection Wizard Setup

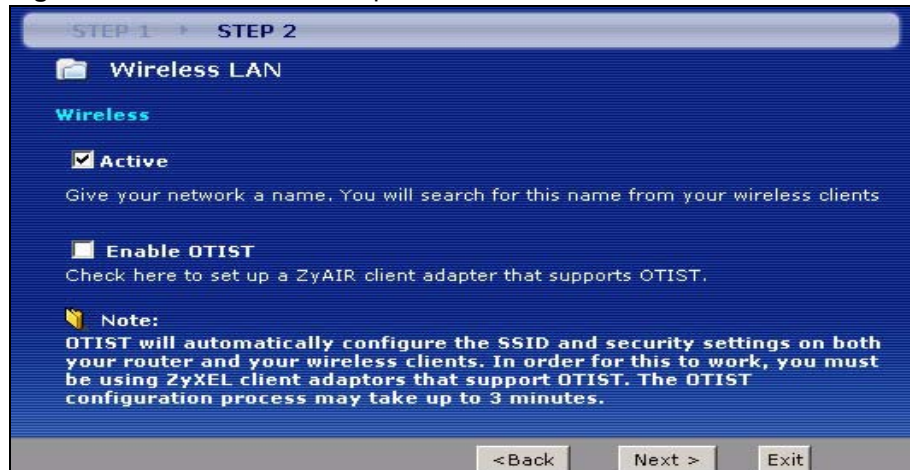
After you configure the Internet access information, use the following screens to set up your wireless LAN.

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



**Figure 21** Connection Test Successful

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

**Figure 22** Wireless LAN Setup Wizard 1

The following table describes the labels in this screen.

**Table 10** Wireless LAN Setup Wizard 1

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

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

**Figure 23** Wireless LAN

The following table describes the labels in this screen.

**Table 11** Wireless LAN Setup Wizard 2

LABEL	DESCRIPTION
Network Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyXEL Device, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device.
Security	Select <b>Automatically assign a WPA key</b> to allow the ZyXEL Device to configure a WPA key for you based on the setup key you entered on the previous screen. This option is only available if you selected <b>Enable OTIST</b> . See <a href="#">Section 3.3.1 on page 63</a> for more information. Select <b>Manually assign a WPA-PSK key</b> to configure a Pre-Shared Key (WPA-PSK). Choose this option only if your wireless clients support WPA. See <a href="#">Section 3.3.2 on page 63</a> for more information. Select <b>Manually assign a WEP key</b> to configure a WEP Key. See <a href="#">Section 3.3.3 on page 63</a> for more information. Select <b>Disable wireless security</b> to have no wireless LAN security configured and your network is accessible to any wireless networking device that is within range.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

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

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

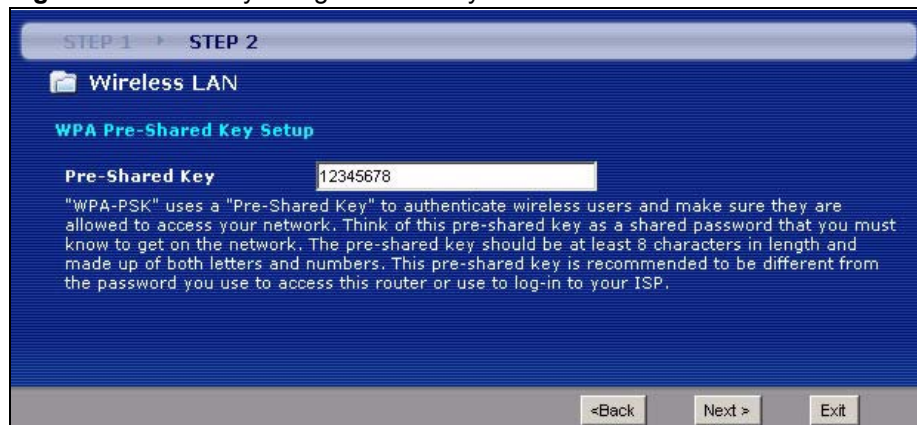
### 3.3.1 Automatically assign a WPA key

Choose **Manually assign a WPA key** in the Wireless LAN setup screen to allow the ZyXEL Device to configure a PSK key for you based on the setup key you entered on the previous Wireless LAN setup screen. This key acts like a password to ensure only those Wireless LAN devices you authorize are configured by OTIST.

### 3.3.2 Manually Assign a WPA key

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

**Figure 24** Manually Assign a WPA key



The following table describes the labels in this screen.

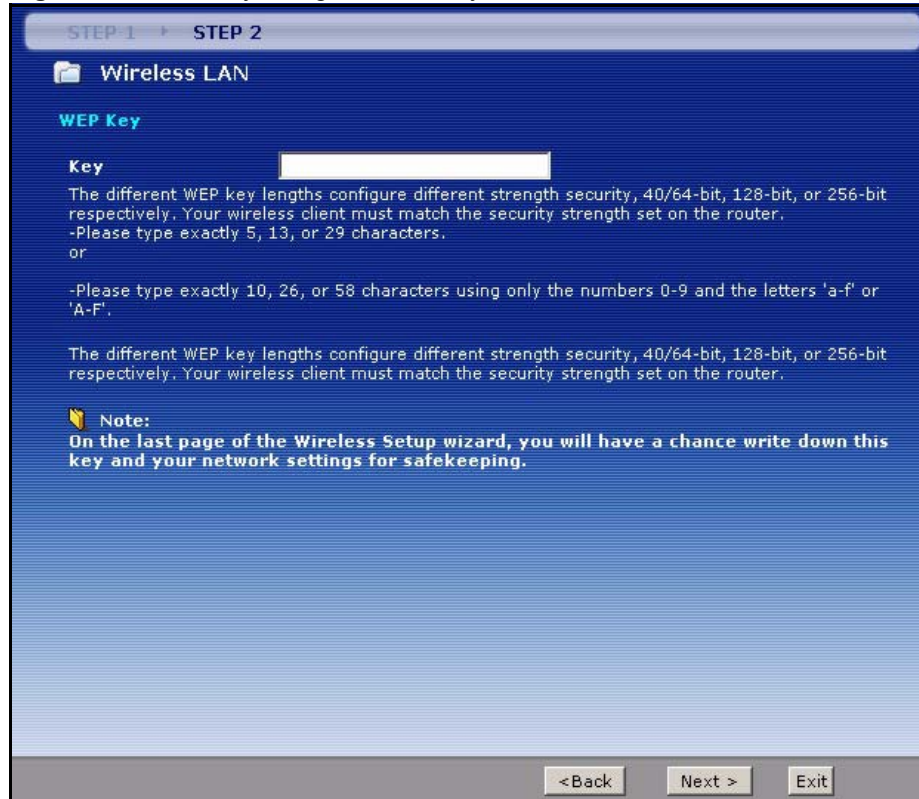
**Table 12** Manually Assign a WPA key

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

### 3.3.3 Manually Assign a WEP key

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

**Figure 25** Manually Assign a WEP key

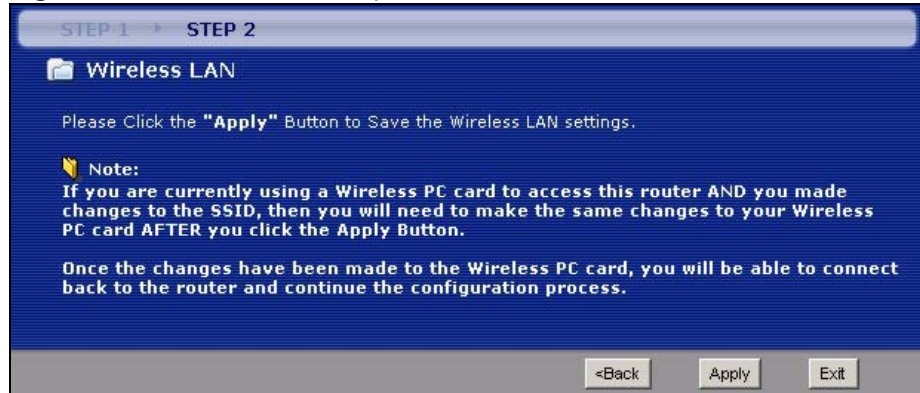


The following table describes the labels in this screen.

**Table 13** Manually Assign a WEP key

LABEL	DESCRIPTION
Key	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. Enter any 5, 13 or 29 ASCII characters or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

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

**Figure 26** Wireless LAN Setup 3

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

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

**Figure 27** Internet Access and WLAN Wizard Setup Complete

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



# CHAPTER 4

## VoIP Wizard And Example

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

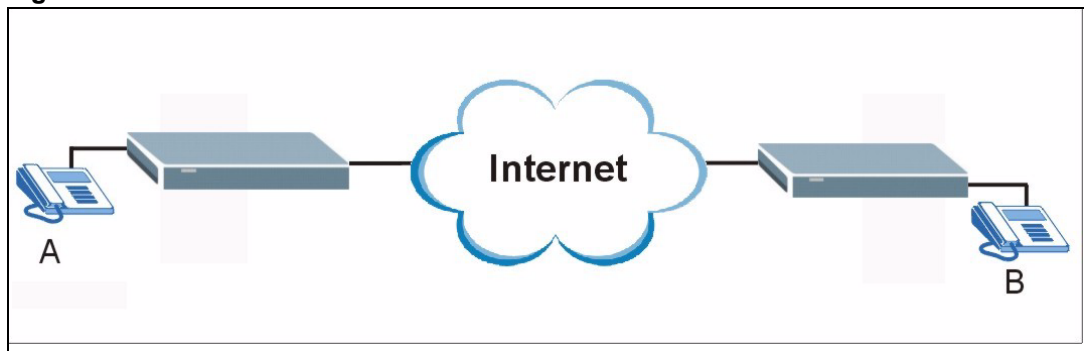
### 4.1 Introduction

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

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


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

**Figure 28** VoIP Phone Calls



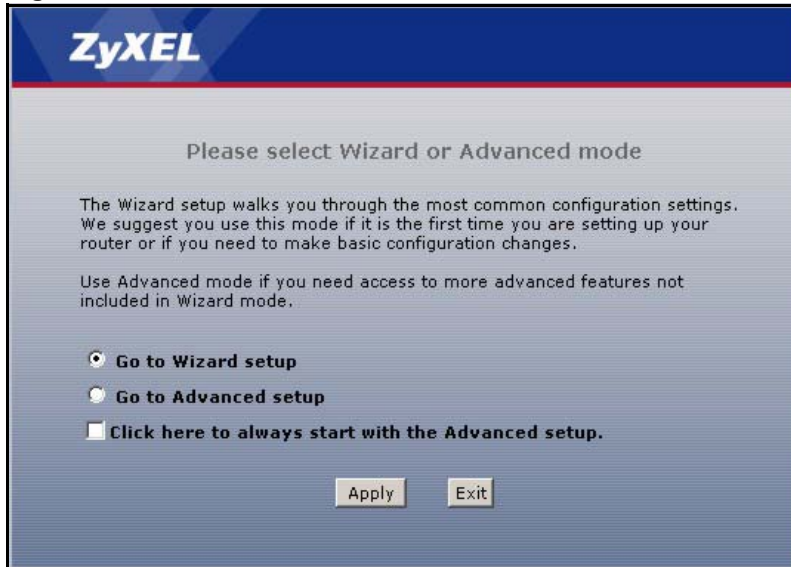
In order to make VoIP calls you need to register at least one SIP account on your ZyXEL Device. You can register your SIP account in the **VOICE OVER INTERNET SETUP** wizard.

### 4.2 VoIP Wizard Setup

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



**Figure 29** Select a Mode



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

**Figure 30** Wizard: Welcome





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

**Table 14** Sample SIP Account Information

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

**Figure 31** VoIP Wizard Configuration

The following table describes the labels in this screen.

**Table 15** VoIP Wizard Configuration

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

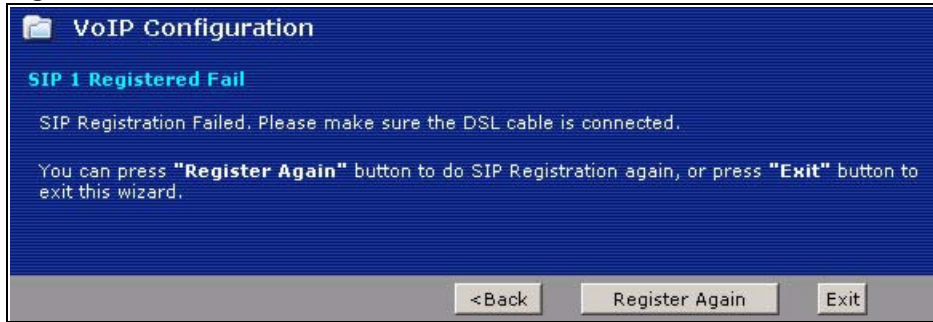
**Table 15** VoIP Wizard Configuration

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

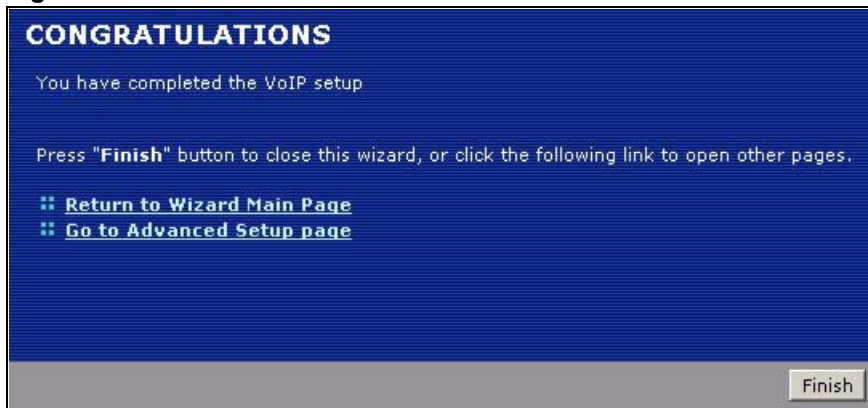
- 4 Your ZyXEL Device will attempt to register your SIP account with your VoIP service provider. When your account is registered your **PHONE 1** light will come on and you are ready to make and receive VoIP phone calls.

**Figure 32** SIP Registration Test

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

**Figure 33** VoIP Wizard Fail

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

**Figure 34** VoIP Wizard Finish

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

You can also use your VoIP service provider's dialing plan to call regular phone numbers. You dial a prefix number, provided to you by your VoIP service provider, followed by a regular phone number.

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



# CHAPTER 5

## Bandwidth Management Wizard

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

### 5.1 Introduction

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

### 5.2 Predefined Media Bandwidth Management Services

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


**Table 16** Media Bandwidth Management Setup: Services

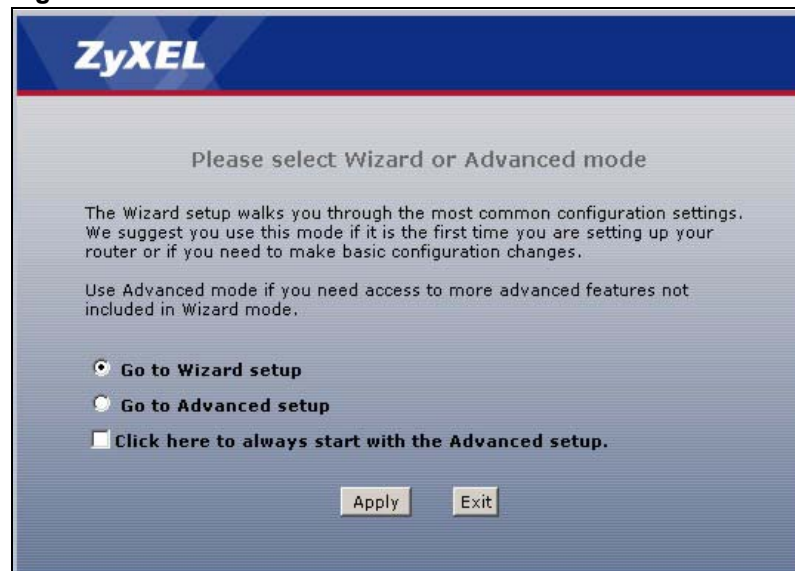
SERVICE	DESCRIPTION
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses TCP (Transmission Control Protocol) port number 21.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. Telnet uses TCP port 23.

**Table 16** Media Bandwidth Management Setup: Services (continued)

SERVICE	DESCRIPTION
NetMeeting (H.323)	A multimedia communications product from Microsoft that enables groups to teleconference and videoconference over the Internet. NetMeeting supports VoIP, text chat sessions, a whiteboard, and file transfers and application sharing. NetMeeting uses H.323. H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. H.323 is transported primarily over TCP, using the default port number 1720.
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.
VoIP (H.323)	Sending voice signals over the Internet is called Voice over IP or VoIP. H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. H.323 is transported primarily over TCP, using the default port number 1720.
TFTP	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).

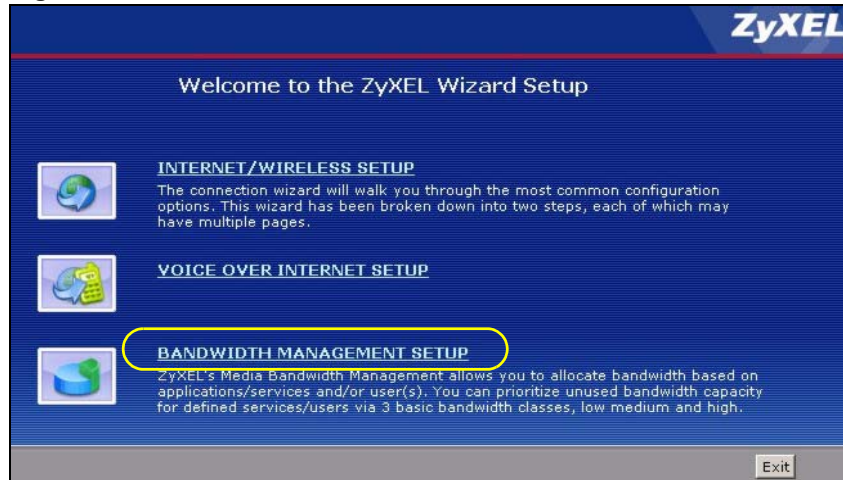
## 5.3 Bandwidth Management Wizard Setup

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

**Figure 35** Select a Mode

## 2 Click **BANDWIDTH MANAGEMENT SETUP**.

**Figure 36** Wizard: Welcome



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

**Figure 37** Bandwidth Management Wizard: General Information



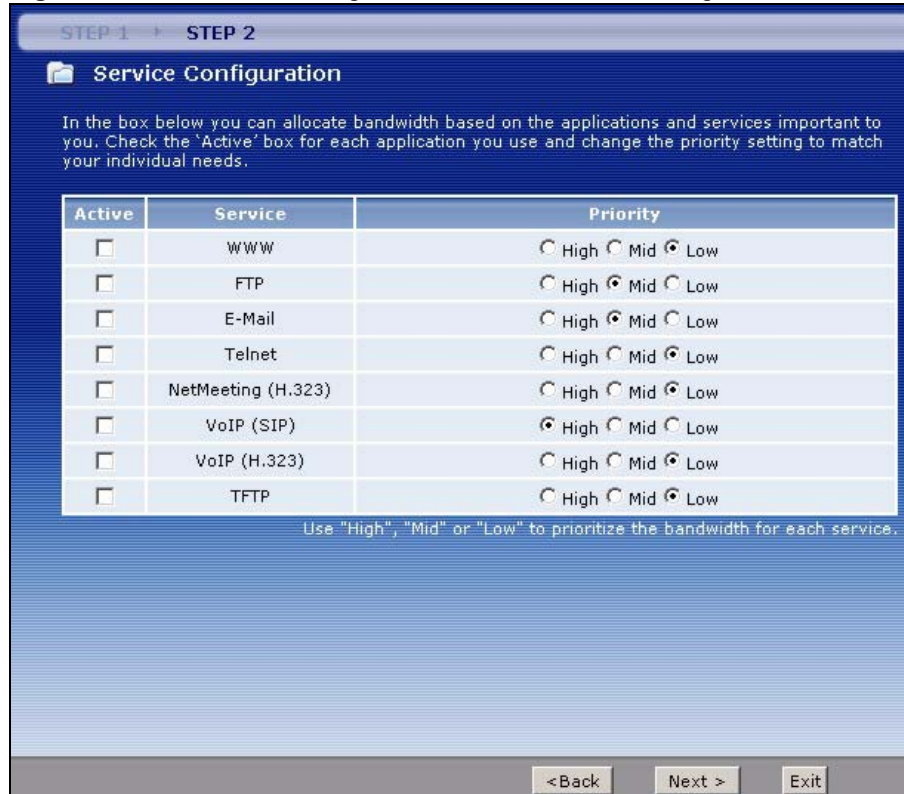
The following fields describe the label in this screen.

**Table 17** Bandwidth Management Wizard: General Information

LABEL	DESCRIPTION
Active	Select the <b>Active</b> check box to have the ZyXEL Device apply bandwidth management to traffic going out through the ZyXEL Device's WAN, LAN or WLAN port. Select <b>Auto Classifier</b> to automatically allocate bandwidth to packets based on the packet size or <b>Services Setup</b> to allocate bandwidth based on the service requirements.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

- 4 Use the next wizard screen to select the services that you want to apply bandwidth management and select the priorities that you want to apply to the services listed.

**Figure 38** Bandwidth Management Wizard: Service Configuration



The following table describes the labels in this screen.

**Table 18** Bandwidth Management Wizard: Service Configuration

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



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

**Figure 39** Bandwidth Management Wizard: Complete





# CHAPTER 6

## Status Screens

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

### 6.1 Status Screen

Click **Status** to open this screen.

**Figure 40** Status Screen

The screenshot displays the Status Screen with a 'Refresh Interval' of 5 seconds and an 'Apply' button. It is divided into several sections:

- Device Information:**
  - Host Name: [111](#)
  - Model Number: P-2608HWL-D1
  - MAC Address: 00:13:49:00:00:01
  - ZyNOS Firmware Version: [V3.40\(ADT.0\)a1\\_0213\\_1](#)
  - DSL Firmware Version: [01/27/2006](#)
  - DSL Information:
    - DSL Mode: NORMAL
    - IP Address: [0.0.0.0](#)
    - IP Subnet Mask: 0.0.0.0
    - Default Gateway: 0.0.0.0
    - VPI/VCI: 0/33
  - LAN Information:
    - IP Address: [192.168.1.1](#)
    - IP Subnet Mask: 255.255.255.0
    - DHCP: [Server](#)
  - WLAN Information:
    - SSID: [ZyXEL](#)
    - Channel: 6
    - Security: Disable
  - Security:
    - Firewall: [Disable](#)
    - Content Filter: [Disable](#)
- System Status:**
  - System Uptime: 2:17:12
  - Current Date/Time: 01/05/2000 01:27:57
  - System Mode: [Routing / Bridging](#)
  - CPU Usage: 2.62%
  - Memory Usage: 22%
- Interface Status:**

Interface	Status	Rate
DSL	Down	0 kbps / 0 kbps
LAN	Up	100M/Full Duplex
WLAN	Active	54M
- Summary:**
  - [Client List](#)
  - [WLAN Status](#)
  - [VPN Status](#)
  - [VoIP Statistics](#)
  - [AnyIP Table](#)
  - [Bandwidth Status](#)
  - [Packet Statistics](#)
- VoIP Status:**

Account	Registration	URI
SIP 1	<a href="#">Register</a> Register Fail	ChangeMe@127.0.0.1
SIP 2	<a href="#">Register</a> Inactive	ChangeMe@127.0.0.1
SIP 3	<a href="#">Register</a> Inactive	
SIP 4	<a href="#">Register</a> Inactive	
SIP 5	<a href="#">Register</a> Inactive	
SIP 6	<a href="#">Register</a> Inactive	
SIP 7	<a href="#">Register</a> Inactive	
SIP 8	<a href="#">Register</a> Inactive	

Each field is described in the following table.

**Table 19** Status Screen

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

**Table 19** Status Screen

LABEL	DESCRIPTION
Security	
Firewall	This displays whether or not the ZyXEL Device's firewall is activated. Click this to go to the screen where you can change it.
Content Filter	This displays whether or not the ZyXEL Device's content filtering is activated. Click this to go to the screen where you can change it.
System Status	
System Uptime	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it ( <b>Maintenance &gt; Tools &gt; Restart</b> ), or when you reset it (see <a href="#">Section 2.1.2 on page 48</a> ).
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in <b>Maintenance &gt; System &gt; Time Setting</b> .
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management; see <a href="#">Chapter 21 on page 277</a> ).
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.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.
Status	<p>For the DSL interface, this field displays <b>Down</b> (line is down), <b>Up</b> (line is up or connected) if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Up</b> (line is up or connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation.</p> <p>This field indicates whether or not the ZyXEL Device is using the interface.</p> <p>For the LAN interface, this field displays <b>Up</b> when the ZyXEL Device is using the interface and <b>Down</b> when the ZyXEL Device is not using the interface.</p> <p>For the WLAN interface, it displays <b>Active</b> when WLAN is enabled or <b>Inactive</b> when WLAN is disabled.</p>
Rate	<p>For the LAN interface, this displays the port speed and duplex setting.</p> <p>For the DSL interface, it displays the downstream and upstream transmission rate.</p> <p>For the WLAN interface, it displays the transmission rate when WLAN is enabled or <b>N/A</b> when WLAN is disabled.</p>
Summary	
Client List	Click this link to view current DHCP client information. See <a href="#">Section 8.5 on page 114</a> .
AnyIP Table	Click this link to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the ZyXEL Device. See <a href="#">Section 6.2 on page 82</a> .
WLAN Status	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device. See <a href="#">Section 6.3 on page 83</a> .
Bandwidth Status	Click this link to view the ZyXEL Device's bandwidth usage and allotments. See <a href="#">Section 21.10 on page 287</a> .

**Table 19** Status Screen

LABEL	DESCRIPTION
VPN Status	Click this link to view the ZyXEL Device's current VPN connections. See <a href="#">Section 18.6 on page 243</a> .
Packet Statistics	Click this link to view port status and packet specific statistics. See <a href="#">Section 6.4 on page 83</a> .
VoIP Statistics	Click this link to view statistics about your VoIP usage. See <a href="#">Section 6.5 on page 85</a> .
VoIP Status	
Account	This column displays each SIP account in the ZyXEL Device.
Registration	<p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p>If the SIP account is already registered with the SIP server,</p> <ul style="list-style-type: none"> <li>Click <b>Unregister</b> to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name.</li> <li>The second field displays <b>Registered</b>.</li> </ul> <p>If the SIP account is not registered with the SIP server,</p> <ul style="list-style-type: none"> <li>Click <b>Register</b> to have the ZyXEL Device attempt to register the SIP account with the SIP server.</li> <li>The second field displays the reason the account is not registered.</li> </ul> <p><b>Inactive</b> - The SIP account is not active. You can activate it in <b>VoIP &gt; SIP &gt; SIP Settings</b>.</p> <p><b>Register Fail</b> - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.</p>
URI	This field displays the account number and service domain of the SIP account. You can change these in <b>VoIP &gt; SIP &gt; SIP Settings</b> .

## 6.2 Any IP Table

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

**Figure 41** Any IP Table

AnyIP Table		
#	IP Address	MAC Address
Refresh		

Each field is described in the following table.

**Table 20** Any IP Table

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

## 6.3 WLAN Status

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

**Figure 42** WLAN Status

Wireless LAN- Association List		
#	MAC Address	Association Time
001	00:03:7f:be:32:01	00:54:22 2000/01/01

Refresh

The following table describes the labels in this screen.

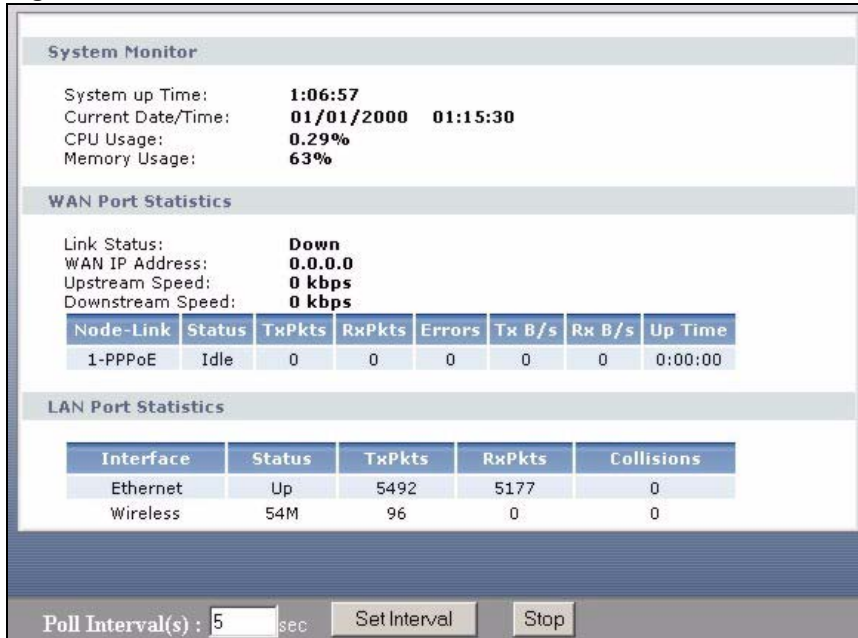
**Table 21** WLAN Status

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

## 6.4 Packet Statistics

Click **Status > Packet Statistics** to access this screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

**Figure 43** Packet Statistics



The following table describes the fields in this screen.

**Table 22** Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
WAN Port Statistics	
Link Status	This is the status of your WAN link.
WAN IP Address	This is the IP address of the ZyXEL Device's WAN port.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Status	This field displays <b>Down</b> (line is down), <b>Up</b> (line is up or connected) if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Up</b> (line is up or connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.



**Table 22** Packet Statistics (continued)

LABEL	DESCRIPTION
Up Time	This field displays the elapsed time this port has been up.
LAN Port Statistics	
Interface	This field displays either <b>Interface</b> (LAN ports) or <b>Wireless</b> (WLAN port).
Status	For the LAN ports, this field displays <b>Down</b> (line is down) or <b>Up</b> (line is up or connected). For the WLAN port, it displays the transmission rate when WLAN is enabled or <b>N/A</b> when WLAN is disabled.
TxPkts	This field displays the number of packets transmitted on this interface.
RxPkts	This field displays the number of packets received on this interface.
Collisions	This is the number of collisions on this interfaces.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this to apply the new poll interval you entered in the <b>Poll Interval</b> field above.
Stop	Click this button to halt the refreshing of the system statistics.

## 6.5 VoIP Statistics

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

**Figure 44** VoIP Statistics

SIP Status:							
Account	Registration	Last Registration	URI	Protocol	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP1	Register Fail	N/A	ChangeMe@127.0.0.1	UDP	No	N/A	N/A
SIP2	Inactive	N/A	ChangeMe@127.0.0.1	UDP	No	N/A	N/A
SIP3	Inactive	N/A		UDP	No	N/A	N/A
SIP4	Inactive	N/A		UDP	No	N/A	N/A
SIP5	Inactive	N/A		UDP	No	N/A	N/A
SIP6	Inactive	N/A		UDP	No	N/A	N/A
SIP7	Inactive	N/A		UDP	No	N/A	N/A
SIP8	Inactive	N/A		UDP	No	N/A	N/A

Call Statistics:									
Phone	Hook	Status	Codec	Peer Number	Duration	TxPkts	RxPkts	Tx B/s	Rx B/s
Phone1	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone2	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone3	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone4	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone5	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone6	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone7	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone8	On	N/A	N/A	N/A	0:00:00	0	0	0	0

Poll Interval(s) : 30 sec	Set Interval	Stop
---------------------------	--------------	------

Each field is described in the following table.

**Table 23** VoIP Statistics

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.
Registration	<p>This field displays the current registration status of the SIP account. You can change this in the <b>Status</b> screen.</p> <p><b>Registered</b> - The SIP account is registered with a SIP server.</p> <p><b>Register Fail</b> - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.</p> <p><b>Inactive</b> - The SIP account is not active. You can activate it in <b>VoIP &gt; SIP &gt; SIP Settings</b>.</p>
Last Registration	This field displays the last time you successfully registered the SIP account. It displays <b>N/A</b> if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in <b>VoIP &gt; SIP &gt; SIP Settings</b> .
Protocol	This field displays the transport protocol the SIP account uses. SIP accounts always use UDP.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. It displays <b>N/A</b> if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. It displays <b>N/A</b> if the SIP account has never dialed a number.
Call Statistics	
Phone	This field displays each phone port in the ZyXEL Device.
Hook	<p>This field indicates whether the phone is on the hook or off the hook.</p> <p><b>On</b> - The phone is hanging up or already hung up.</p> <p><b>Off</b> - The phone is dialing, calling, or connected.</p>
Status	<p>This field displays the current state of the phone call.</p> <p><b>N/A</b> - There are no current VoIP calls, incoming calls or outgoing calls being made.</p> <p><b>DIAL</b> - The callee's phone is ringing.</p> <p><b>RING</b> - The phone is ringing for an incoming VoIP call.</p> <p><b>Process</b> - There is a VoIP call in progress.</p> <p><b>DISC</b> - The callee's line is busy, the callee hung up or your phone was left off the hook.</p>
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Duration	This field displays how long the current call has lasted.
Tx Pkts	This field displays the number of packets the ZyXEL Device has transmitted in the current call.
Rx Pkts	This field displays the number of packets the ZyXEL Device has received in the current call.

**Table 23** VoIP Statistics

LABEL	DESCRIPTION
Tx B/s	This field displays how quickly the ZyXEL Device has transmitted packets in the current call. The rate is the average number of bytes transmitted per second.
Rx B/s	This field displays how quickly the ZyXEL Device has received packets in the current call. The rate is the average number of bytes transmitted per second.
Poll Interval(s)	Enter how often you want the ZyXEL Device to update this screen, and click <b>Set Interval</b> .
Set Interval	Click this to make the ZyXEL Device update the screen based on the amount of time you specified in <b>Poll Interval</b> .
Stop	Click this to make the ZyXEL Device stop updating the screen.



# CHAPTER 7

## WAN Setup

This chapter describes how to configure WAN settings.

### 7.1 WAN Overview

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

#### 7.1.1 Encapsulation

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

##### 7.1.1.1 ENET ENCAP

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

##### 7.1.1.2 PPP over Ethernet

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

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

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

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

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

### **7.1.1.3 PPPoA**

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

### **7.1.1.4 RFC 1483**

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

## **7.1.2 Multiplexing**

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

### **7.1.2.1 VC-based Multiplexing**

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

### **7.1.2.2 LLC-based Multiplexing**

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

## **7.1.3 VPI and VCI**

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

## 7.1.4 IP Address Assignment

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

### 7.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation

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

### 7.1.4.2 IP Assignment with RFC 1483 Encapsulation

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

### 7.1.4.3 IP Assignment with ENET ENCAP Encapsulation

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

## 7.1.5 Nailed-Up Connection (PPP)

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

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

## 7.1.6 NAT

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

## 7.2 Metric

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

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

- Normal route: designated by the ISP (see [Section 7.5 on page 94](#))
- Traffic-redirect route (see [Section 7.7 on page 102](#))
- WAN-backup route, also called dial-backup (see [Section 7.8 on page 103](#))

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

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

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

## 7.3 Traffic Shaping

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

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

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

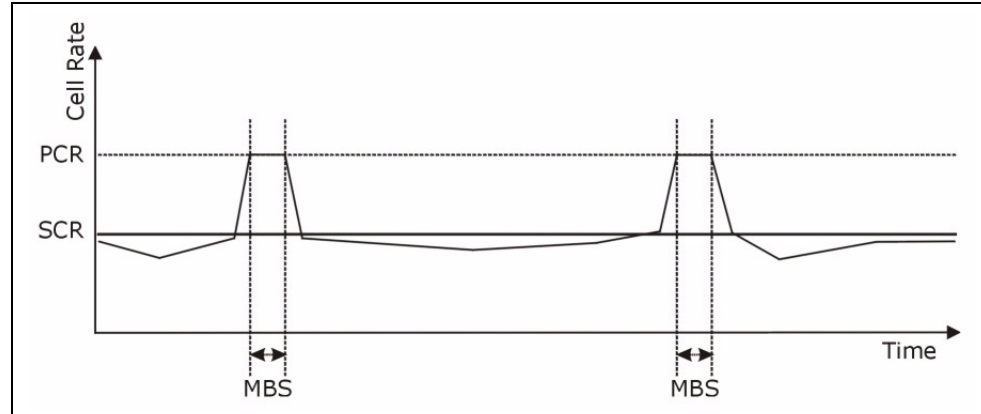


Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

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

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

**Figure 45** Example of Traffic Shaping



## 7.3.1 ATM Traffic Classes

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

### 7.3.1.1 Constant Bit Rate (CBR)

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

### 7.3.1.2 Variable Bit Rate (VBR)

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

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

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

### 7.3.1.3 Unspecified Bit Rate (UBR)

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

## 7.4 Zero Configuration Internet Access

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

Zero configuration for Internet access is disabled when

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

## 7.5 Internet Access Setup

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

See [Section 7.1 on page 89](#) for more information.

**Figure 46** Internet Access Setup (PPPoE)

The following table describes the labels in this screen.

**Table 24** Internet Access Setup

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

**Table 24** Internet Access Setup (continued)

LABEL	DESCRIPTION
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are <b>VC</b> or <b>LLC</b> .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	<p>This option is available if you select <b>Routing</b> in the <b>Mode</b> field.</p> <p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.</p> <p>Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the <b>IP Address</b> field below.</p>
Subnet Mask (ENET ENCAP encapsulation only)	<p>Enter a subnet mask in dotted decimal notation.</p> <p>Refer to the appendix to calculate a subnet mask if you are implementing subnetting.</p>
Gateway IP address (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select <b>ENET ENCAP</b> in the <b>Encapsulation</b> field
DNS Server	
First DNS Server Second DNS Server Third DNS Server	<p>Select <b>Obtained From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address).</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>DNS Relay</b> to have the ZyXEL Device act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The ZyXEL Device's LAN IP address displays in the field to the right (read-only). The ZyXEL Device tells the DHCP clients on the LAN that the ZyXEL Device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select <b>DNS Relay</b> for a second or third DNS server, that choice changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.

**Table 24** Internet Access Setup (continued)

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

## 7.5.1 Advanced Internet Access Setup

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

**Figure 47** Advanced Internet Access Setup

The following table describes the labels in this screen.

**Table 25** Advanced Internet Access Setup

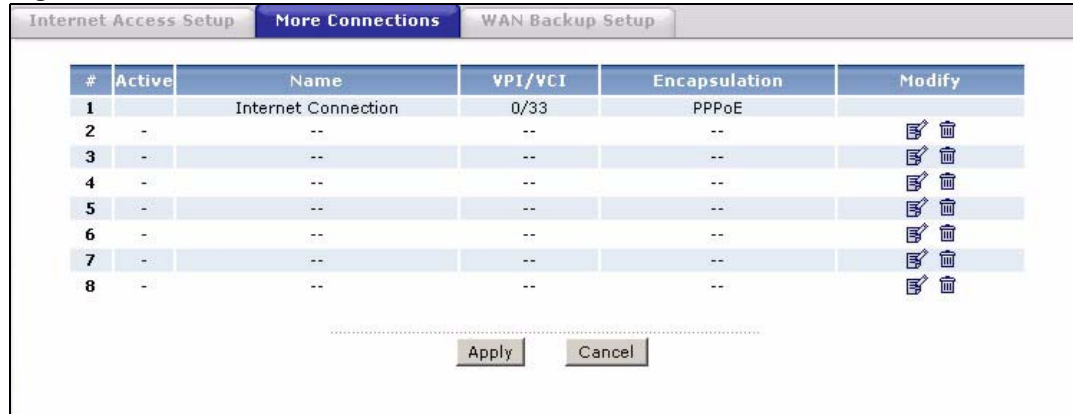
LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer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

**Table 25** Advanced Internet Access Setup (continued)

LABEL	DESCRIPTION
ATM QoS Type	Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select <b>UBR</b> (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select <b>VBR-RT</b> (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select <b>VBR-nRT</b> (non real-time Variable Bit Rate) type for connections that do not require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Zero Configuration	This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode. Select <b>Yes</b> to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes. Select <b>No</b> to disable this feature. You must manually configure the ZyXEL Device for Internet access.
PPPoE Passthrough (PPPoE encapsulation only)	This field is available when you select <b>PPPoE</b> encapsulation. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 7.6 WAN More Connections

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

**Figure 48** WAN More Connections

The following table describes the labels in this screen.

**Table 26** WAN More Connections

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

### 7.6.1 WAN More Connections Modify Screen

Use this screen to modify or create additional WAN connections. Click the **Modify** icon in the **Network > WAN > More Connections** screen to edit your WAN connections.

**Figure 49** WAN More Connections > Modify

General	
<input checked="" type="checkbox"/> Active	
Name	ChangeMe
Mode	Routing
Encapsulation	PPPoE
User Name	ZyXEL
Password	*****
Service Name	
Multiplexing	VC
VPI	0
VCI	33
IP Address	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.0.1
Connection	
<input type="radio"/> Nailed-Up Connection	
<input checked="" type="radio"/> Connect on Demand	
Max Idle timeout	0 sec
NAT	
<input type="radio"/> None	
<input checked="" type="radio"/> SUA Only <a href="#">Edit Detail</a>	
<input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>	

The following table describes the labels in this screen.

**Table 27** WAN More Connections > Modify

LABEL	DESCRIPTION
General	
Active	Use this checkbox to activate or deactivate this WAN connection.
Name	Give a name to this WAN connection. This is for descriptive purposes only.
Mode	Select <b>Routing</b> (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select <b>Bridge</b> .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the <b>Mode</b> field. If you select <b>Bridge</b> in the <b>Mode</b> field, select either <b>PPPoA</b> or <b>RFC 1483</b> . If you select <b>Routing</b> in the <b>Mode</b> field, select <b>PPPoA</b> , <b>RFC 1483</b> , <b>ENET ENCAP</b> or <b>PPPoE</b> .
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.



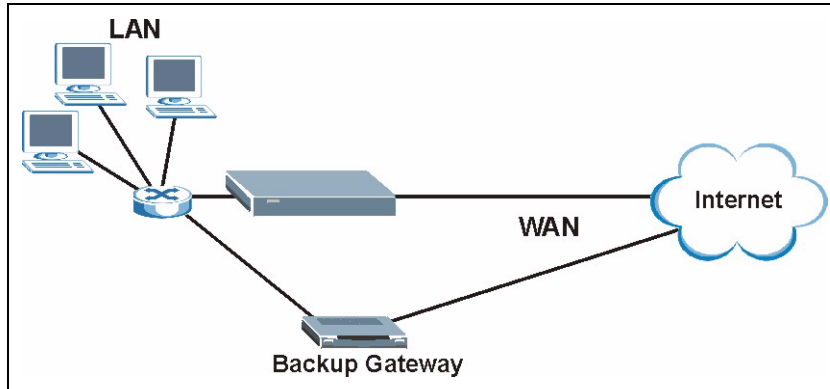
**Table 27** WAN More Connections > Modify (continued)

LABEL	DESCRIPTION
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are <b>VC</b> or <b>LLC</b> .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	This option is available if you select <b>Routing</b> in the <b>Mode</b> field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the <b>IP Address</b> field below.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask If you are implementing subnetting.
Gateway IP address (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select <b>ENET ENCAP</b> in the <b>Encapsulation</b> field
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.
Max Idle Timeout	Specify an idle time-out in the <b>Max Idle Timeout</b> field when you select <b>Connect on Demand</b> . The default setting is 0, which means the Internet session will not timeout.
NAT	Use this section to activate NAT for this connection.
None	Select this if you don't want this WAN connection to use NAT.
SUA Only	Select this to use Single User Account NAT settings, then click <b>Edit Detail</b> to configure your settings. See <a href="#">Section 10.1 on page 139</a> for more details.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click this button to display the <b>Advanced Setup</b> screen and edit more details of your additional WAN connections. See <a href="#">Section 7.5.1 on page 97</a> for more information on this screen.

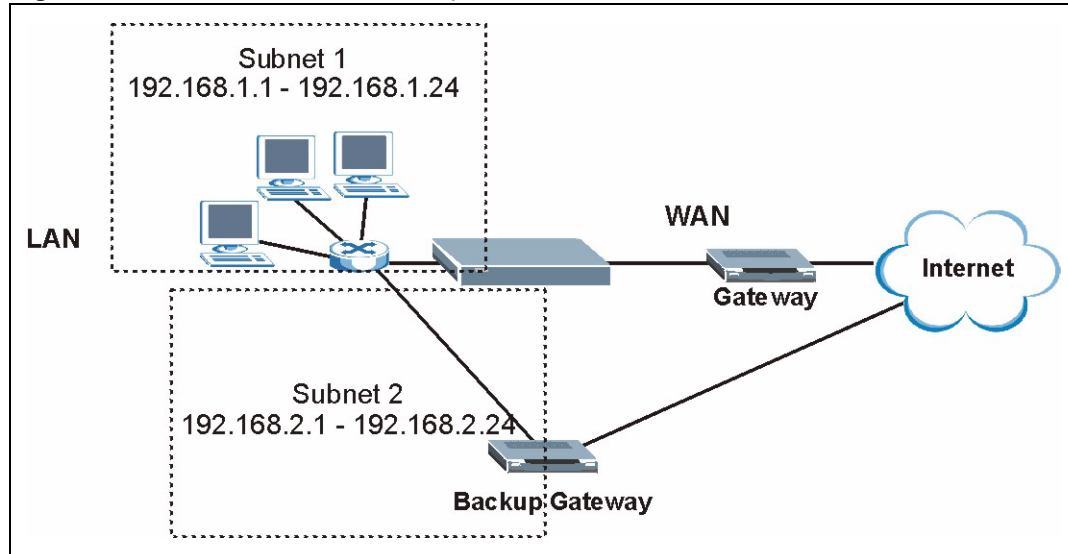
## 7.7 Traffic Redirect

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

**Figure 50** Traffic Redirect Example



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

**Figure 51** Traffic Redirect LAN Setup

## 7.8 WAN Backup Setup

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

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

The following table describes the labels in this screen.

**Table 28** WAN Backup Setup

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

# CHAPTER 8

## LAN Setup

This chapter describes how to configure LAN settings.

### 8.1 LAN Overview

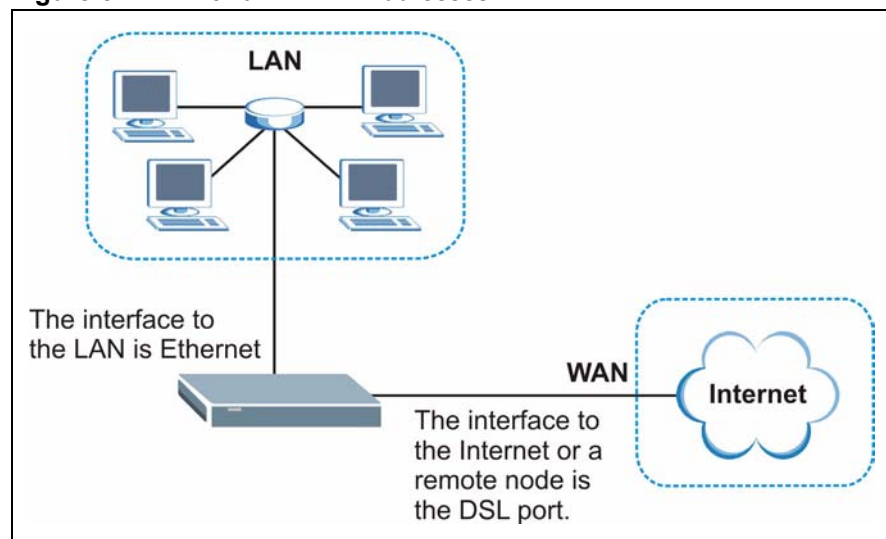
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 8.3 on page 111](#) to configure the LAN screens.

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

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

**Figure 52** LAN and WAN IP Addresses



## 8.1.2 DHCP Setup

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

### 8.1.2.1 IP Pool Setup

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

### 8.1.3 DNS Server Address

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

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

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

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

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

## 8.1.4 DNS Server Address Assignment

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

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

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

## 8.2 LAN TCP/IP

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

### 8.2.1 IP Address and Subnet Mask

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

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

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

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

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

### 8.2.1.1 Private IP Addresses

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

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

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

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

### 8.2.2 RIP Setup

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

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

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

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



### 8.2.3 Multicast

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

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

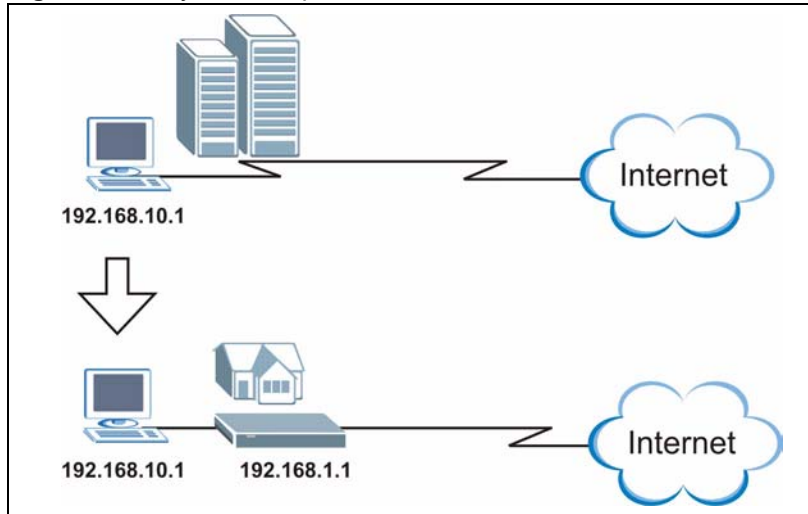
The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on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

### 8.2.4 Any IP

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

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

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

**Figure 53** Any IP Example

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

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

### 8.2.4.1 How Any IP Works

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

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

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

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

## 8.3 Configuring LAN IP

Click **Network > LAN** to open the **IP** screen. See [Section 8.1 on page 105](#) for background information.

**Figure 54** LAN IP

The following table describes the fields in this screen.

**Table 29** LAN IP

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

### 8.3.1 Configuring Advanced LAN Setup

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

**Figure 55** Advanced LAN Setup

The following table describes the labels in this screen.

**Table 30** Advanced LAN Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.
Any IP Setup	Select the <b>Active</b> check box to enable the Any IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.  When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyXEL Device's LAN IP address can connect to the ZyXEL Device or access the Internet through the ZyXEL Device.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.  Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 8.4 DHCP Setup

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

**Figure 56** DHCP Setup

The following table describes the labels in this screen.

**Table 31** DHCP Setup

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

**Table 31** DHCP Setup

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select <b>Obtained From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . Select <b>DNS Relay</b> to have the ZyXEL Device act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The ZyXEL Device's LAN IP address displays in the field to the right (read-only). The ZyXEL Device tells the DHCP clients on the LAN that the ZyXEL Device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select <b>DNS Relay</b> for a second or third DNS server, that choice changes to <b>None</b> after you click <b>Apply</b> . Select <b>None</b> if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.5 LAN Client List

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

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

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

**Figure 57** LAN Client List

The screenshot shows the 'Client List' configuration page. At the top, there are tabs for 'IP', 'DHCP Setup', 'Client List', and 'IP Alias'. Below the tabs is the 'DHCP Client Table' section. It includes input fields for 'IP Address' (192.168.1.66) and 'MAC Address' (AA:BB:CC:EE:EE:EE) with an 'Add' button. The table has the following data:

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

At the bottom of the table, there are three buttons: 'Apply', 'Cancel', and 'Refresh'.

The following table describes the labels in this screen.

**Table 32** LAN Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click <b>Add</b> to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)).
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Refresh	Click <b>Refresh</b> to reload the DHCP table.

## 8.6 LAN IP Alias

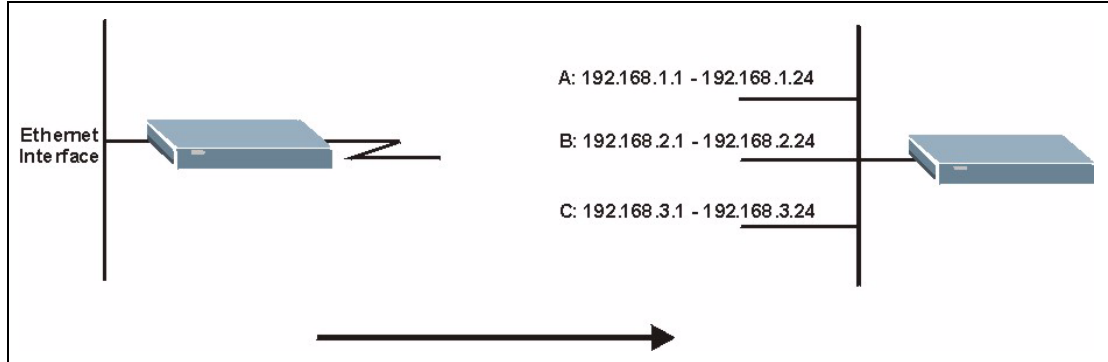
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

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

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

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

**Figure 58** Physical Network & Partitioned Logical Networks



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

**Figure 59** LAN IP Alias

The screenshot shows the 'IP Alias' configuration page in a web interface. At the top, there are tabs for 'IP', 'DHCP Setup', 'Client List', and 'IP Alias'. The main content area is divided into two sections: 'IP Alias 1' and 'IP Alias 2'. Each section contains:
 

- A checkbox to enable the IP alias (currently unchecked).
- An 'IP Address' text input field containing '0.0.0.0'.
- An 'IP Subnet Mask' text input field containing '0.0.0.0'.
- A 'RIP Direction' dropdown menu set to 'None'.
- A 'RIP Version' dropdown menu set to 'N/A'.

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

The following table describes the labels in this screen.

**Table 33** LAN IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.



**Table 33** LAN IP Alias

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyXEL Device will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). <b>RIP-1</b> 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 <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 9

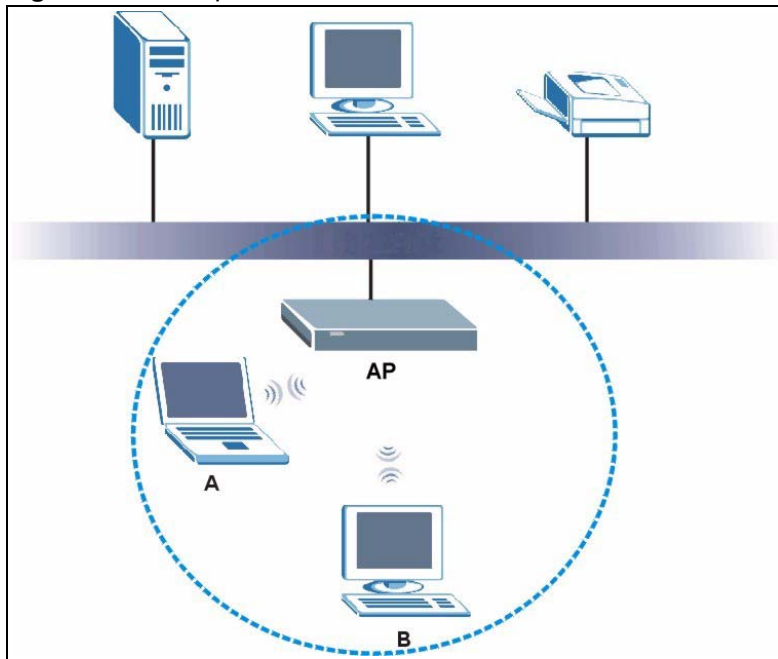
## Wireless LAN

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

### 9.1 Wireless Network Overview

The following figure provides an example of a wireless network.

**Figure 60** Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the 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 device in the same wireless network must use the same SSID.  
The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.  
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.

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

## 9.2 Wireless Security Overview

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

### 9.2.1 SSID

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

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

### 9.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.<sup>1</sup> A MAC address is usually written using twelve hexadecimal characters<sup>2</sup>; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

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

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

### 9.2.3 User Authentication

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

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

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

## 9.2.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See [section 9.2.3 on page 120](#) for information about this.)

**Table 34** Types of Encryption for Each Type of Authentication

	No Authentication	RADIUS Server
<b>Weakest</b>	No Security	WPA WPA2
	Static WEP	
	WPA-PSK	
<b>Strongest</b>	WPA2-PSK	

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

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

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

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

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

### 9.2.5 One-Touch Intelligent Security Technology (OTIST)

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

The devices in the wireless network have to support OTIST, and they have to be in range of the ZyXEL Device when you activate it. See [section 9.6 on page 130](#) for more details.

## 9.3 Wireless Performance Overview

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

### 9.3.1 Quality of Service (QoS)

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

## 9.4 Additional Wireless Terms

The following table describes wireless network terms and acronyms used in the ZyXEL Device.

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.</p>
Preamble	<p>A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.</p>

TERM	DESCRIPTION
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Max. Frame Burst	Enable this to improve the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time that the ZyXEL Device transmits IEEE 802.11g wireless traffic only.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.
Roaming	If you have two or more ZyXEL Devices (or other wireless access points) on your wireless network, you can enable this option so that wireless devices can change locations without having to log in again. This is useful for devices, such as notebooks, that move around a lot.

## 9.5 General Wireless LAN Screen

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

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

**Figure 61** Wireless LAN: General

The screenshot shows the 'Wireless LAN: General' configuration page. At the top, there are four tabs: 'General' (selected), 'OTTIST', 'MAC Filter', and 'QoS'. Below the tabs, the page is divided into two main sections: 'Wireless Setup' and 'Security'. In the 'Wireless Setup' section, the 'Active Wireless LAN' checkbox is checked. The 'Network Name(SSID)' field contains the text 'ZyXEL'. The 'Hide SSID' checkbox is unchecked. The 'Channel Selection' dropdown menu is set to 'Channel-06 2437MHz'. In the 'Security' section, the 'Security Mode' dropdown menu is set to 'No Security'. At the bottom of the page, there are three buttons: 'Apply', 'Cancel', and 'Advanced Setup'.

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

**Table 35** Wireless LAN: General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN.
Network Name(SSID)	<p>(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p> <p><b>Note:</b> If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.</p>
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
Security Mode	See the following sections for more details about this field.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Advanced Setup	Click <b>Advanced Setup</b> to display the <b>Wireless Advanced Setup</b> screen and edit more details of your WLAN setup.

### 9.5.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

**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 62** Wireless: No Security

The screenshot shows a web-based configuration interface for a wireless network. At the top, there are four tabs: 'General' (selected), 'OTIST', 'MAC Filter', and 'QoS'. Below the tabs is a 'Wireless Setup' section with the following options:
 

- Active Wireless LAN
- Network Name(SSID): ZyXEL
- Hide SSID
- Channel Selection: Channel-06 2437MHz

 Below this is a 'Security' section with:
 

- Security Mode: No Security

 At the bottom of the screen are three buttons: 'Apply', 'Cancel', and 'Advanced Setup'.

The following table describes the labels in this screen.

**Table 36** Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose <b>No Security</b> from the drop-down list box.

## 9.5.2 WEP Encryption Screen

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

**Figure 63** Wireless: Static WEP Encryption

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

**Table 37** Wireless: Static WEP Encryption

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

### 9.5.3 WPA(2)-PSK

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

**Figure 64** Wireless: WPA(2)-PSK

The screenshot shows the configuration interface for Wireless LAN security. It is divided into two main sections: 'Wireless Setup' and 'Security'. In the 'Wireless Setup' section, the 'Active Wireless LAN' checkbox is checked, the 'Network Name (SSID)' is set to 'ZyXEL', 'Hide SSID' is unchecked, and 'Channel Selection' 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 timers are configured: 'ReAuthentication Timer' at 1800 seconds, 'Idle Timeout' at 3600 seconds, and 'Group Key Update Timer' at 1800 seconds. At the bottom, there are three buttons: 'Apply', 'Cancel', and 'Advanced Setup'.

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

**Table 38** Wireless: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose <b>WPA-PSK</b> or <b>WPA2-PSK</b> from the drop-down list box.
WPA Compatible	This field is only available for WPA2-PSK. Select this if you want the ZyXEL Device to support WPA-PSK and WPA2-PSK simultaneously.
Pre-Shared Key	The encryption mechanisms used for <b>WPA(2)</b> and <b>WPA(2)-PSK</b> are the same. The only difference between the two is that <b>WPA(2)-PSK</b> uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).  <b>Note:</b> If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
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. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA(2)-PSK</b> key management) or <b>RADIUS</b> server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in <b>WPA-PSK</b> mode. The ZyXEL Device default is 1800 seconds (30 minutes).

## 9.5.4 WPA(2) Authentication Screen

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

**Figure 65** Wireless: WPA(2)

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

**Table 39** Wireless: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose <b>WPA</b> or <b>WPA2</b> from the drop-down list box.
WPA Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.
ReAuthentication Timer (in seconds)	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. The default time interval is 1800 seconds (30 minutes).  <b>Note:</b> If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

**Table 39** Wireless: WPA(2)

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. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The WPA Group Key Update Timer is the rate at which the AP (if using <b>WPA-PSK</b> key management) or <b>RADIUS</b> server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the WPA <b>Group Key Update Timer</b> is also supported in <b>WPA-PSK</b> mode. The ZyXEL Device default is <b>1800</b> seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server (optional)	
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.

### 9.5.5 Wireless LAN Advanced Setup

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

**Figure 66** Advanced

The following table describes the labels in this screen.

**Table 40** Wireless LAN: Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Enter a value between 0 and 2432. If you select the G+ Enhanced checkbox a value of 4096 is displayed.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. If you select the G+ Enhanced checkbox a value of 4096 is displayed.
Preamble	Select a preamble type from the drop-down list menu. Choices are <b>Long</b> , <b>Short</b> or <b>Dynamic</b> . The default setting is <b>Long</b> . See the appendix for more information.
802.11 Mode	Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select <b>Mixed</b> to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Enable 802.11g+ mode	Select <b>Enable 802.11g+ mode</b> checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the ZyXEL Device at higher transmission speeds. This permits the ZyXEL Device to transmit at a higher speed than the <b>802.11g Only</b> mode.
Back	Click this to return to the previous screen without saving changes.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 9.6 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 67** Network > Wireless LAN > OTIST

The screenshot shows the 'OTIST' configuration page. At the top, there are four tabs: 'General', 'OTIST', 'MAC Filter', and 'QoS'. The 'OTIST' tab is selected. Below the tabs, the page title 'OTIST' is displayed. There is a 'Setup Key' label followed by a text input field containing '01234567'. Below this is a checked checkbox with the label 'Yes!' and the text: 'Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a random PSK key for your convenience.' At the bottom center, there is a 'Start' button.

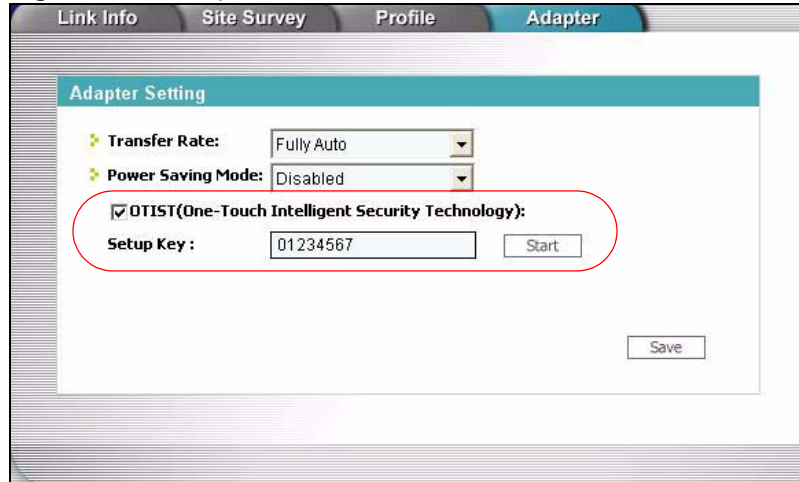
The following table describes the labels in this screen.

**Table 41** Network > Wireless LAN > OTIST

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

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

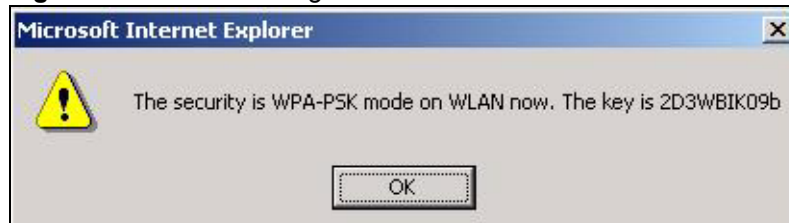
- 1 Start the ZyXEL utility
- 2 Click the **Adapter** tab.
- 3 Select the **OTIST** check box, and enter the same **Setup Key** as the ZyXEL Device.
- 4 Click **Save**.

**Figure 68** Example: Wireless Client OTIST Screen

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

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

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

**Figure 69** OTIST: Settings

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

Review the settings, and click **OK**. The following screen displays on the web configurator.

**Figure 70** OTIST In Progress Screen on the ZyXEL Device



The following screen appears on the wireless client.

**Figure 71** OTIST: In Progress on the Wireless Device

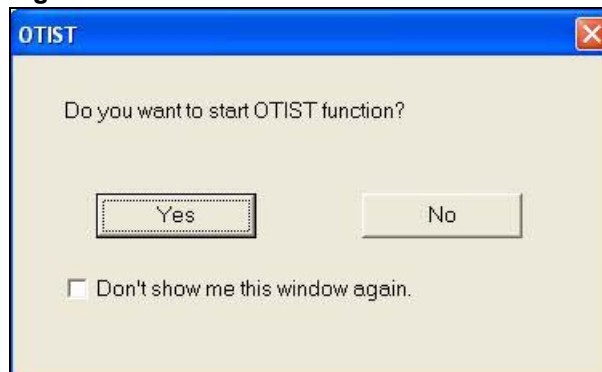


These screens close when the transfer is complete.

### 9.6.1 Notes on OTIST

- 1 If you enable OTIST in a wireless device, 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 72** Start OTIST?



- 2 If an OTIST-enabled wireless device 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 device 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 device 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 Devices after using OTIST, you need to run OTIST again or enter them manually in the wireless device(s).
- 5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless device joins your wireless network, you need to run OTIST on the AP and ALL wireless devices again.

## 9.7 MAC Filter

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

**Figure 73** MAC Address Filter

General DTIST **MAC Filter** QoS

MAC Filter

Active MAC Filter

Filter Action  Allow  Deny

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

Apply Cancel

The following table describes the labels in this menu.

**Table 42** MAC Address Filter

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

**Table 42** MAC Address Filter

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 9.8 QoS Screen

The QoS screen by default allows you to automatically give a service a priority level.

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

Wireless LAN: QoS

QoS

Enable WMM QoS

WMM QoS Policy: Application Priority

#	Name	Service	Dest Port	Priority	Modify
1	-	-	0	-	
2	-	-	0	-	
3	-	-	0	-	
4	-	-	0	-	
5	-	-	0	-	
6	-	-	0	-	
7	-	-	0	-	
8	-	-	0	-	
9	-	-	0	-	
10	-	-	0	-	

Apply Cancel

The following table describes the fields in this screen.

**Table 43** Wireless LAN: QoS

LABEL	DESCRIPTION
QoS	
Enable WMM QoS	Select the check box to enable WMM QoS on the ZyXEL Device.
WMM QoS Policy	Select <b>Default</b> to have the ZyXEL Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. Select <b>Application Priority</b> from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
	This table only appears if you select <b>Application Priority</b> in <b>WMM QoS Policy</b> .
#	This is the number of an individual application entry.

**Table 43** Wireless LAN: QoS

LABEL	DESCRIPTION
Name	This field displays a description given to an application entry.
Service	This field displays either <b>FTP</b> , <b>WWW</b> , <b>E-mail</b> or a <b>User Defined</b> service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.
Priority	This field displays the WMM QoS priority for traffic bandwidth.
Modify	Click the <b>Edit</b> icon to open the <b>Application Priority Configuration</b> screen. Modify an existing application entry or create a application entry in the <b>Application Priority Configuration</b> screen. Click the <b>Remove</b> icon to delete an application entry.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.

### 9.8.1 Application Priority Configuration

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

**Figure 74** Application Priority Configuration

See [Appendix A on page 387](#) for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

**Table 44** Application Priority Configuration

LABEL	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.

**Table 44** Application Priority Configuration

LABEL	DESCRIPTION
Service	<p>The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box.</p> <ul style="list-style-type: none"> <li>• <b>FTP</b> File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.</li> <li>• <b>E-Mail</b> 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</li> <li>• <b>WWW</b> The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.</li> <li>• <b>User-Defined</b> User-defined services are user specific services configured using known ports and applications.</li> </ul>
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previous screen.



# CHAPTER 10

## Network Address Translation (NAT) Screens

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

### 10.1 NAT Overview

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

#### 10.1.1 NAT Definitions

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

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

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

**Table 45** NAT Definitions

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

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

## 10.1.2 What NAT Does

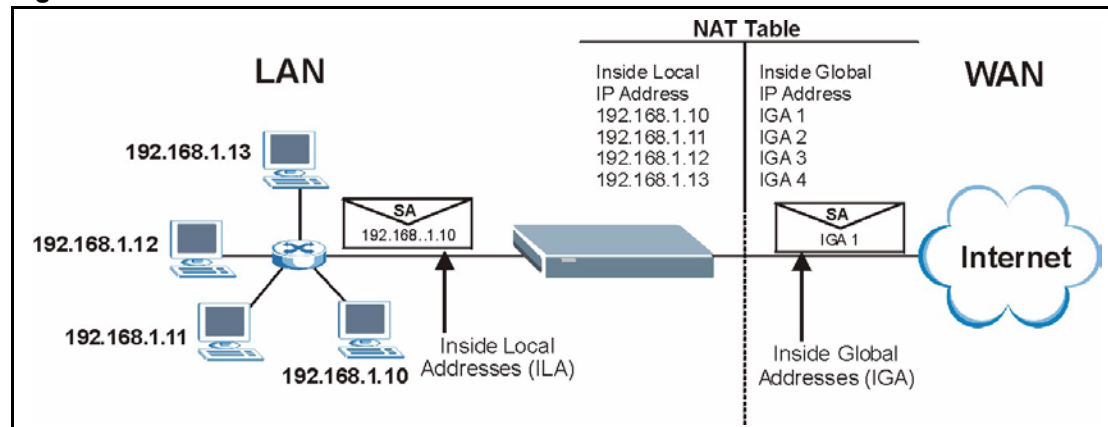
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 46 on page 142](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

## 10.1.3 How NAT Works

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

**Figure 75** How NAT Works

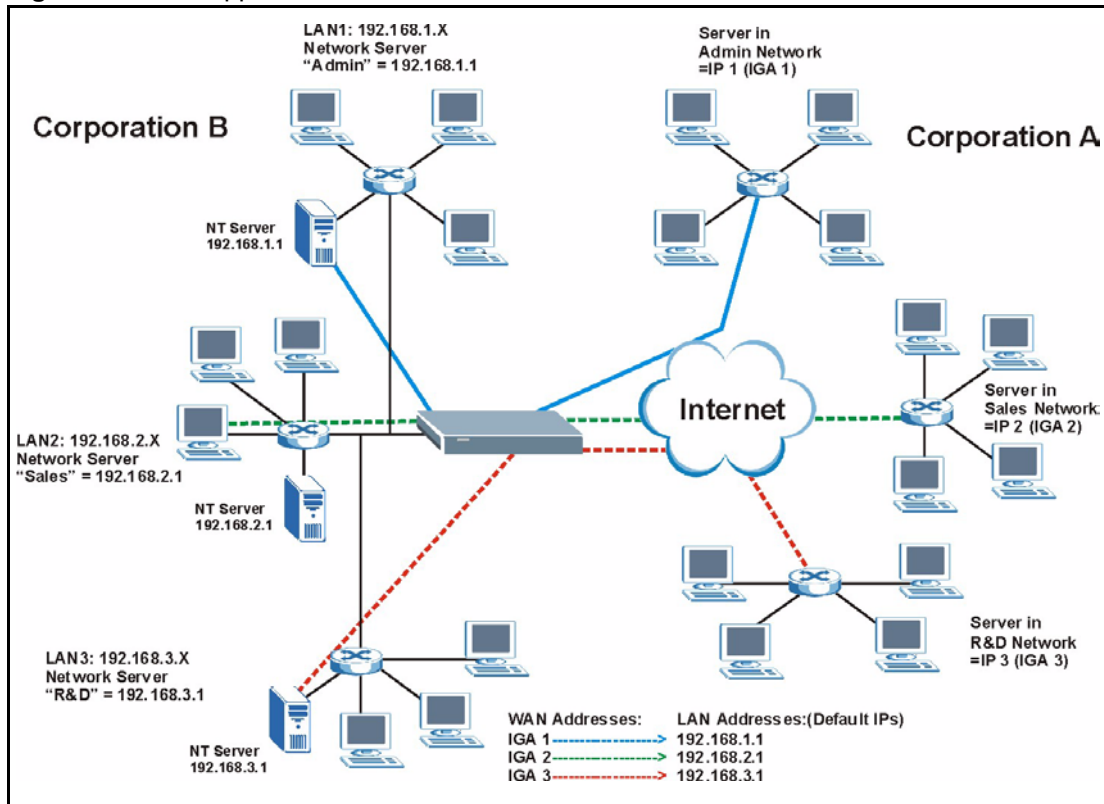




## 10.1.4 NAT Application

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

**Figure 76** NAT Application With IP Alias



## 10.1.5 NAT Mapping Types

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

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

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

The following table summarizes these types.

**Table 46** NAT Mapping Types

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

## 10.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 46 on page 142](#).

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

## 10.3 NAT General Setup

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

**Figure 77** NAT General

The following table describes the labels in this screen.

**Table 47** NAT General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Max NAT/ Firewall Session Per User	When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.  Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/Firewall sessions client computers can establish through the ZyXEL Device.  If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is exhausting all of the available NAT sessions.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 10.4 Port Forwarding

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

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

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

### 10.4.1 Default Server IP Address

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

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

### 10.4.2 Port Forwarding: Services and Port Numbers

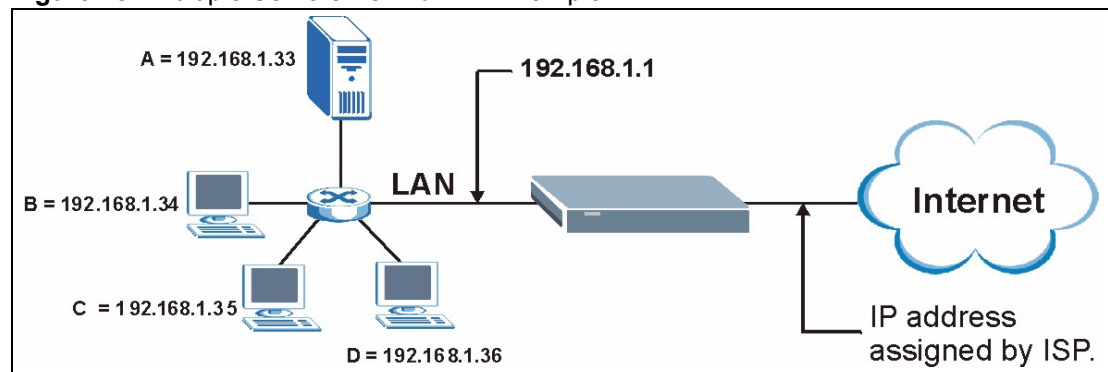
Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers and services are shown in [Appendix D on page 387](#). Please refer to RFC 1700 for further information about port numbers.

### 10.4.3 Configuring Servers Behind Port Forwarding (Example)

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

**Figure 78** Multiple Servers Behind NAT Example



## 10.5 Configuring Port Forwarding

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

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

See [Appendix D on page 387](#) for port numbers commonly used for particular services.

**Figure 79** Port Forwarding

The following table describes the fields in this screen.

**Table 48** Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a <b>Default Server</b> IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	Click this check box to enable the rule.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Server IP Address	This is the server's IP address.

**Table 48** Port Forwarding

LABEL	DESCRIPTION
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previous configuration.

## 10.5.1 Port Forwarding Rule Edit

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

**Figure 80** Port Forwarding Rule Setup

The following table describes the fields in this screen.

**Table 49** Port Forwarding Rule Setup

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the <b>End Port</b> field. To forward a series of ports, enter the start port number here and the end port number in the <b>End Port</b> field.
End Port	Enter a port number in this field. To forward only one port, enter the port number again in the <b>Start Port</b> field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the <b>Start Port</b> field above.
Server IP Address	Enter the inside IP address of the server here.
Back	Click <b>Back</b> to return to the previous screen.

**Table 49** Port Forwarding Rule Setup (continued)

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

## 10.6 Address Mapping

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

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

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

**Figure 81** 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 50** Address Mapping Rules

LABEL	DESCRIPTION
#	This is the rule index number.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.

**Table 50** Address Mapping Rules (continued)

LABEL	DESCRIPTION
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-one</b> and <b>Server</b> mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for <b>Many-to-One</b> and <b>Server</b> mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is <b>N/A</b> for <b>One-to-one</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Type	<p><b>1-1:</b> One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p><b>M-1:</b> Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</p> <p><b>M-M Ov (Overload):</b> Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p><b>MM No (No Overload):</b> Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p><b>Server:</b> This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

## 10.6.1 Address Mapping Rule Edit

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

**Figure 82** Edit Address Mapping Rule

The screenshot shows a web form titled "Edit Address Mapping Rule1". The form contains the following fields and controls:

- Type:** A dropdown menu currently 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".
- Server Mapping Set:** A dropdown menu set to "N/A" with a blue "Edit Details" link to its right.

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



The following table describes the fields in this screen.

**Table 51** Edit Address Mapping Rule

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <ul style="list-style-type: none"> <li>• <b>One-to-One:</b> One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.</li> <li>• <b>Many-to-One:</b> Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</li> <li>• <b>Many-to-Many Overload:</b> Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</li> <li>• <b>Many-to-Many No Overload:</b> Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</li> <li>• <b>Server:</b> This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</li> </ul>
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Server Mapping Set	Only available when <b>Type</b> is set to <b>Server</b> . Select a number from the drop-down menu to choose a server mapping set.
Edit Details	Click this link to go to the <b>Port Forwarding</b> screen to edit a server mapping set that you have selected in the <b>Server Mapping Set</b> field.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.6.2 SIP ALG

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your ZyXEL Device is behind a SIP ALG.

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

**Figure 83** Network > NAT > ALG

The screenshot shows a web interface for configuring ALG settings. At the top, there are three tabs: 'General', 'Port Forwarding', and 'ALG'. The 'ALG' tab is active. Below the tabs is a section titled 'ALG Settings'. Inside this section, there is a checkbox labeled 'Enable SIP ALG' which is checked. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

Each field is described in the following table.

**Table 52** Network > NAT > ALG

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

# CHAPTER 11

## SIP

Use these screens to set up your SIP accounts and to configure QoS settings.

### 11.1 SIP Overview

#### 11.1.1 Introduction to VoIP

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

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

#### 11.1.2 Introduction to SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

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

#### 11.1.3 SIP Identities

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

##### 11.1.3.1 SIP Number

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

### 11.1.3.2 SIP Service Domain

The SIP service domain of the VoIP service provider (the company that lets you make phone calls over the Internet) is the domain name in a SIP URI. For example, if the SIP address is [1122334455@VoIP-provider.com](mailto:1122334455@VoIP-provider.com), then “VoIP-provider.com” is the SIP service domain.

### 11.1.4 SIP Call Progression

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

**Table 53** SIP Call Progression

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

A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.

- 6** B sends a response indicating that the telephone is ringing.
- 7** B sends an OK response after the call is answered.
- 8** A then sends an ACK message to acknowledge that B has answered the call.
- 9** Now A and B exchange voice media (talk).
- 10** After talking, A hangs up and sends a BYE request.
- 11** B replies with an OK response confirming receipt of the BYE request and the call is terminated.

### 11.1.5 SIP Client Server

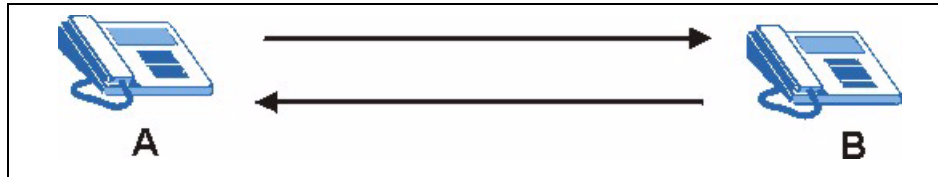
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

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

### 11.1.5.1 SIP User Agent

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

**Figure 84** SIP User Agent



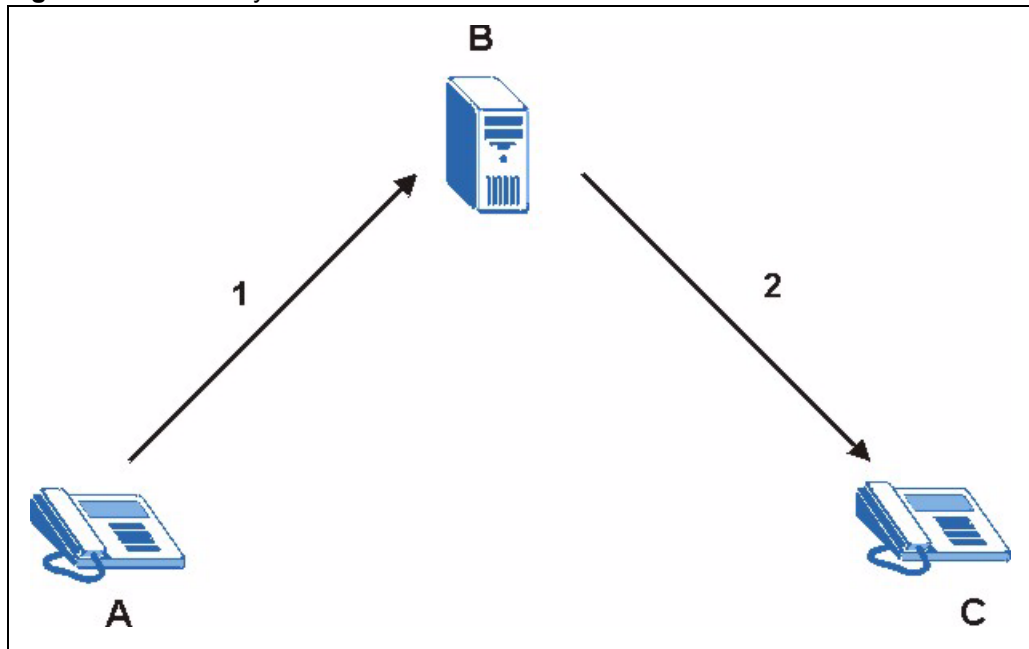
### 11.1.5.2 SIP Proxy Server

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

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

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

**Figure 85** SIP Proxy Server



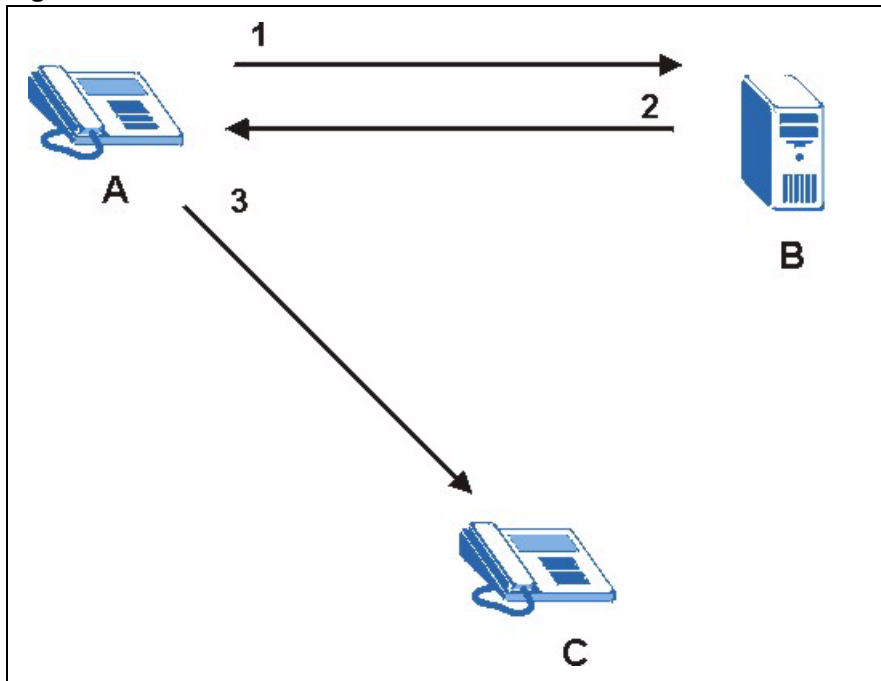
### 11.1.5.3 SIP Redirect Server

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

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

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

**Figure 86** SIP Redirect Server



### 11.1.5.4 SIP Register Server

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

### 11.1.6 RTP

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

## 11.1.7 NAT and SIP

The ZyXEL Device must register its public IP address with a SIP register server. If there is a NAT router between the ZyXEL Device and the SIP register server, the ZyXEL Device probably has a private IP address. The ZyXEL Device lists its IP address in the SIP message that it sends to the SIP register server. NAT does not translate this IP address in the SIP message. The SIP register server gets the ZyXEL Device's IP address from inside the SIP message and maps it to your SIP identity. If the ZyXEL Device has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity. See [Chapter 10 on page 139](#) for more information about NAT.

Use a SIP ALG (Application Layer Gateway), use NAT, STUN, or outbound proxy to allow the ZyXEL Device to list its public IP address in the SIP messages.

### 11.1.7.1 SIP ALG

See [Section 10.6.2 on page 149](#).

### 11.1.7.2 Use NAT

If you know the NAT router's public IP address and SIP port number, you can use the Use NAT feature to manually configure the ZyXEL Device to use them in the SIP messages. This eliminates the need for STUN or a SIP ALG.

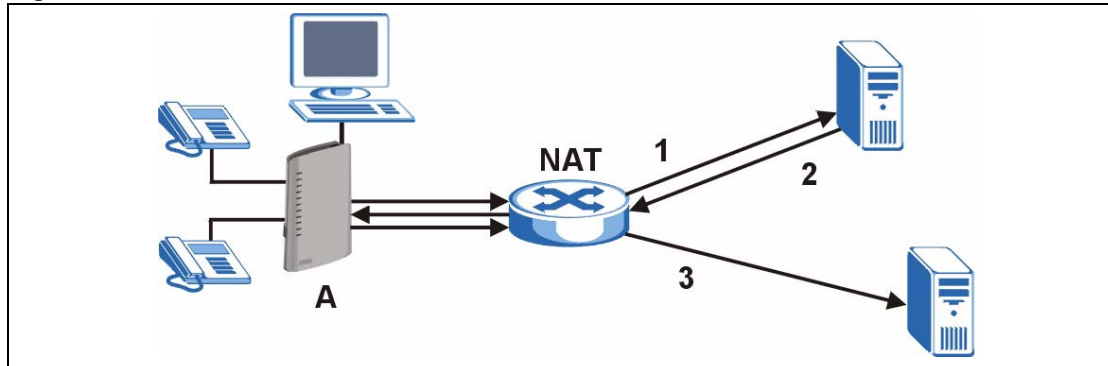
You must also configure the NAT router to forward traffic with this port number to the ZyXEL Device.

### 11.1.7.3 STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the ZyXEL Device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the ZyXEL Device to find the public IP address that NAT assigned, so the ZyXEL Device can embed it in the SIP data stream. STUN does not work with symmetric NAT routers or firewalls. See RFC 3489 for details on STUN.

The following figure shows how STUN works.

- 1 The ZyXEL Device (A) sends SIP packets to the STUN server (B).
- 2 The STUN server (B) finds the public IP address and port number that the NAT router used on the ZyXEL Device's SIP packets and sends them to the ZyXEL Device.
- 3 The ZyXEL Device uses the public IP address and port number in the SIP packets that it sends to the SIP server (C).

**Figure 87** STUN

#### 11.1.7.4 Outbound Proxy

Your VoIP service provider may host a SIP outbound proxy server to handle all of the ZyXEL Device's VoIP traffic. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the ZyXEL Device to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).

#### 11.1.8 Voice Coding

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

- **G.711** is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into bits. G.711 provides very good sound quality but requires 64kbps of bandwidth.
- **G.729** is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

#### 11.1.9 PSTN Call Setup Signaling

PSTNs (Public Switched Telephone Networks) use DTMF or pulse dialing to set up telephone calls.

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

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

1. The ZyXEL Device supports DTMF at the time of writing.



### 11.1.10 MWI (Message Waiting Indication)

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

### 11.1.11 Custom Tones (IVR)

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

**Table 54** Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	120 seconds for all custom tones combined
Time per Individual Tone	20 seconds
Total Number of Tones Recordable	8 You can record up to 8 different custom tones but the total time must be 120 seconds or less.

#### 11.1.11.1 Recording Custom Tones

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

- 1 Pick up the phone and press “\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1101~1108 on your phone followed by the “#” key.
- 3 Play your desired music or voice recording into the receiver’s mouthpiece. Press the “#” key.
- 4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

#### 11.1.11.2 Listening to Custom Tones

Do the following to listen to a custom tone:

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

#### 11.1.11.3 Deleting Custom Tones

Do the following to delete a custom tone:

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

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

## 11.1.12 Quality of Service (QoS)

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

### 11.1.12.1 Type Of Service (ToS)

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

### 11.1.12.2 DiffServ

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

### 11.1.12.3 DSCP and Per-Hop Behavior

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

**Figure 88** DiffServ: Differentiated Service Field

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

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

---

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

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

#### **11.1.12.4 VLAN**

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

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

## **11.2 SIP Screens**

### **11.2.1 SIP Settings Screen**

Use this screen to maintain basic information about each SIP account. Your VoIP service provider (the company that lets you make phone calls over the Internet) should provide this. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP > SIP Settings**.

**Figure 89** VoIP > SIP > SIP Settings

Each field is described in the following table.

**Table 55** VoIP > SIP > SIP Settings

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

**Table 55** VoIP > SIP > SIP Settings

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

## 11.2.2 Advanced SIP Setup Screen

Use this screen to maintain advanced settings for each SIP account. To access this screen, click **Advanced Setup** in **VoIP > SIP > SIP Settings**.

**Figure 90** VoIP > SIP > SIP Settings > Advanced

SIP Account : SIP1

---

**SIP Server Settings**

URL Type:

Expiration Duration:  (20-65535) sec

Register Re-send timer:  (1-65535) sec

Session Expires:  (30-3600) sec

Min-SE:  (20-1800) sec

---

**RTP Port Range**

Start Port:  (1025-65535)

End Port:  (1025-65535)

---

**Voice Compression**

Primary Compression Type:

Secondary Compression Type:

Third Compression Type:

DTMF Mode:

---

**Outbound Proxy**

Enable

Server Address:

Server Port:  (1025-65535)

---

**MWI (Message Waiting Indication)**

Enable

Expiration Time:  (1-65535) sec

---

**Fax Option**

G.711 Fax Passthrough       T.38 Fax Relay

---

**Call Forward**

Call Forward Table:

---

**Caller Ringing**

Enable

Caller Ringing Tone:

---

**On Hold**

Enable

On Hold Tone:

---

Each field is described in the following table.

**Table 56** VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
SIP Account	This field displays the SIP account you see in this screen.
SIP Server Settings	

**Table 56** VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
URL Type	Select whether or not to include the SIP service domain name when the ZyXEL Device sends the SIP number. <b>SIP</b> - include the SIP service domain name <b>TEL</b> - do not include the SIP service domain name
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The ZyXEL Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the ZyXEL Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the ZyXEL Device accepts.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the <b>Start Port</b> and <b>End Port</b> fields. To enter a range of ports, <ul style="list-style-type: none"> <li>• enter the port number at the beginning of the range in the <b>Start Port</b> field</li> <li>• enter the port number at the end of the range in the <b>End Port</b> field.</li> </ul>
Voice Compression	Select the type of voice coder/decoder (codec) that you want the ZyXEL Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). <ul style="list-style-type: none"> <li>• <b>G.711A</b> is typically used in Europe.</li> <li>• <b>G.711u</b> is typically used in North America and Japan.</li> </ul> In contrast, <b>G.729</b> only requires 8 kbps. The ZyXEL Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.
Primary Compression Type	Select the ZyXEL Device's first choice for voice coder/decoder.
Secondary Compression Type	Select the ZyXEL Device's second choice for voice coder/decoder. Select <b>None</b> if you only want the ZyXEL Device to accept the first choice.
Third Compression Type	Select the ZyXEL Device's third choice for voice coder/decoder. Select <b>None</b> if you only want the ZyXEL Device to accept the first or second choice.
DTMF Mode	Control how the ZyXEL Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. <b>RFC 2833</b> - send the DTMF tones in RTP packets <b>PCM</b> - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. <b>SIP INFO</b> - send the DTMF tones in SIP messages
Outbound Proxy	

**Table 56** VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the ZyXEL Device to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
MWI (Message Waiting Indication)	
Enable	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
Expiration Time	Keep the default value, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the ZyXEL Device subscribes to the service. Before this time passes, the ZyXEL Device automatically subscribes again.
Fax Option	This field controls how the ZyXEL Device handles fax messages.
G.711 Fax Passthrough	Select this if the ZyXEL Device should use G.711 to send fax messages. The peer devices must also use G.711.
T.38 Fax Relay	Select this if the ZyXEL Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have interoperability problems. The peer devices must also use T.38.
Call Forward	
Call Forward Table	Select which call forwarding table you want the ZyXEL Device to use for incoming calls. You set up these tables in <b>VoIP &gt; Phone Book &gt; Incoming Call Policy</b> .
Caller Ringing	
Enable	Select the check box if you want to specify what tone people hear when they call you. The ZyXEL Device provides a default tone, but you can add additional tones using IVR. See <a href="#">Section 11.1.11 on page 157</a> for more information.
Caller Ringing Tone	Select the tone you want people to hear when they call you. You should setup these tones using IVR first. See <a href="#">Section 11.1.11 on page 157</a> for more information.
On Hold	
Enable	Select the check box if you want to specify what tone people hear when you put them on hold. The ZyXEL Device provides a default tone, but you can add additional tones using IVR. See <a href="#">Section 11.1.11 on page 157</a> for more information.
On Hold Tone	Select the tone you want people to hear when you put them on hold. You should setup these tones using IVR first. See <a href="#">Section 11.1.11 on page 157</a> for more information.
Back	Click this to return to the <b>SIP Settings</b> screen without saving your changes.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.



### 11.2.3 SIP QoS Screen

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

**Figure 91** VoIP > SIP > QoS

Each field is described in the following table.

**Table 57** VoIP > SIP > QoS

LABEL	DESCRIPTION
SIP TOS Priority Setting	Enter the priority for SIP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to voice traffic that it transmits.
RTP TOS Priority Setting	Enter the priority for RTP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to RTP traffic that it transmits.
Voice VLAN ID	Select this if the ZyXEL Device has to be a member of a VLAN to communicate with the SIP server. Ask your network administrator, if you are not sure. Enter the VLAN ID provided by your network administrator in the field on the right. Your LAN and gateway must be configured to use VLAN tags. Otherwise, clear this field.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.



# CHAPTER 12

## Phone

Use these screens to configure the phones you use to make phone calls.

### 12.1 Phone Overview

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

#### 12.1.1 Voice Activity Detection/Silence Suppression/Comfort Noise

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

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

#### 12.1.2 Echo Cancellation

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

#### 12.1.3 Supplementary Phone Services Overview

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

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls

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

### 12.1.3.1 The Flash Key

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

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

### 12.1.3.2 Europe Type Supplementary Phone Services

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

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

**Table 58** European Type Flash Key Commands

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

#### 12.1.3.2.1 European Call Hold

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

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

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

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

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

#### **12.1.3.2.2 European Call Waiting**

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

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

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

#### **12.1.3.2.3 European Call Transfer**

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

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

#### **12.1.3.2.4 European Three-Way Conference**

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

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

### 12.1.3.3 USA Type Supplementary Services

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

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

**Table 59** USA Type Flash Key Commands

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

#### 12.1.3.3.1 USA Call Hold

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

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

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

#### 12.1.3.3.2 USA Call Waiting

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

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

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

#### 12.1.3.3.3 USA Call Transfer

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

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

#### 12.1.3.3.4 USA Three-Way Conference

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

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

## 12.2 Phone Screens

Use these screens to configure your phone settings.

### 12.2.1 Analog Phone Screen

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

**Figure 92** VoIP > Phone > Analog Phone

Each field is described in the following table.

**Table 60** VoIP > Phone > Analog Phone

LABEL	DESCRIPTION
Phone Port Settings	Select the phone port you want to see in this screen. If you change this field, the screen automatically refreshes.
Outgoing Call Use	
SIP1 ... SIP8	Select which SIP accounts you want to use for outgoing calls. If you select multiple accounts then the ZyXEL Device will try to use the lower numbered SIP account first.
Incoming Call apply to	
SIP1 ... SIP8	Select which SIP accounts you want to receive phone calls from on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
PSTN Line	Select this if you want to receive phone calls from the PSTN line (that do not use the Internet) on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this phone port. The <b>Advanced Analog Phone Setup</b> screen appears.

## 12.2.2 Advanced Analog Phone Setup Screen

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



**Figure 93** VoIP > Phone > Analog Phone > Advanced

Analog Phone 1

**Voice Volume Control**

Speaking Volume

Listening Volume

**Echo Cancellation**

G.168 Active

**Dialing Interval Select**

Dialing Interval Select

VAD Support

<Back Apply Reset

Each field is described in the following table.

**Table 61** VoIP > Phone > Analog Phone > Advanced

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

## 12.2.3 Common Phone Settings Screen

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

**Figure 94** VoIP > Phone > Common

Each field is described in the following table.

**Table 62** VoIP > Phone > Common

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

## 12.2.4 Phone Region Screen

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

**Figure 95** VoIP > Phone > Region

The screenshot shows a web interface for configuring VoIP settings. At the top, there are three tabs: 'Analog Phone', 'Common', and 'Region'. The 'Region' tab is selected. Below the tabs is a section titled 'Region Settings'. This section contains two dropdown menus: 'Region Settings' with 'Poland' selected, and 'Call Service Mode' with 'Europe Type' selected. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

Each field is described in the following table.

**Table 63** VoIP > Phone > Region

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



# CHAPTER 13

## Phone Book

Use these screens to maintain call-forwarding rules and speed-dial settings.

### 13.1 Phone Book Overview

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers. It is also required if you want to make peer-to-peer calls. In peer-to-peer calls, you call another VoIP device directly without going through a SIP server. In the ZyXEL Device, you must set up a speed dial entry in the phone book in order to do this. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The ZyXEL Device sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

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

### 13.2 Speed Dial Screen

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

**Figure 96** Phone Book > Speed Dial

Each field is described in the following table.

**Table 64** Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
Speed Dial	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the ZyXEL Device to call when you dial the speed-dial number.
Name	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Type	Select <b>Use Proxy</b> if you want to use one of your SIP accounts to call this phone number. Select <b>Non-Proxy (Use IP or URL)</b> if you want to use a different SIP server or if you want to make a peer-to-peer call. In this case, enter the IP address or domain name of the SIP server or the other party in the field below.
Add	Click this to use the information in the <b>Speed Dial</b> section to update the <b>Speed Dial Phone Book</b> section.
Speed Dial Phone Book	Use this section to look at all the speed-dial entries and to erase them.
Speed Dial	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the ZyXEL Device calls when you dial the speed-dial number.
Name	This field displays the name of the party you call when you dial the speed-dial number.

**Table 64** Phone Book > Speed Dial

LABEL	DESCRIPTION
Destination	This field is blank, if the speed-dial entry uses one of your SIP accounts. Otherwise, this field shows the IP address or domain name of the SIP server or other party. (This field corresponds with the <b>Type</b> field in the <b>Speed Dial</b> section.)
Modify	Use this field to edit or erase the speed-dial entry. Click the <b>Edit</b> icon to copy the information for this speed-dial entry into the <b>Speed Dial</b> section, where you can change it. Click the <b>Remove</b> icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Reset	Click this to set every field in this screen to its last-saved value.

## 13.3 Incoming Call Policy Screen

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

**Figure 97** Phone Book > Incoming Call Policy

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

**Table 65** Phone Book > Incoming Call Policy

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



**Table 65** Phone Book > Incoming Call Policy

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

## 13.4 Group Ring Screen

This screen lets you specify ring types for calls from particular numbers. The ring types vary by ring duration and stop ring duration. Any standard phone is compatible with this feature.

When an incoming call comes in, the ZyXEL Device checks if it is from any of the phone numbers you set up in this screen. If the number matches an enabled entry, the ZyXEL Device sends the corresponding ring to your phone. You can also configure different rings for calls coming into various SIP accounts, coming into the PSTN line and internal calls.

To access this screen, click **VoIP > Phone Book > Group Ring**.

**Figure 98** Phone Book > Group Ring

Each field is described in the following table.

**Table 66** Phone Book > Group Ring

LABEL	DESCRIPTION
Active	Select this if you want to activate the group ring feature. You also have to enable individual entries.
Test the Ring	Use the drop down list box to select the ring tone you would like to hear (A-H).
Test	Click this to listen to the ring. All the phones connected to the ZyXEL Device ring when you click this button.
Ring Select	Use this section to first assign rings to groups and then assign phone numbers to those groups.
Family	Select the ring for callers in your family group.
Workmate	Select the ring for callers in your workmate group.
Friend	Select the ring for callers in your friend group.
VIP	Select the ring for callers in your VIP group.
#	This is a read only index number for the phone numbers you assign to different groups.
Enable	Select this to enable your selected group ring for this phone number.

**Table 66** Phone Book > Group Ring

LABEL	DESCRIPTION
Name	Type a name for the associated telephone number.
TEL	Type the telephone number you want to add to a group.
Group	Select a group for the telephone number you entered. You can select <b>Family, Workmate, Friend</b> or <b>VIP</b> .
SIP1-SIP8	You can also assign special rings for the different SIP accounts you have configured on your ZyXEL Device. Select a ring type for each of your configured SIP accounts.  <b>Note:</b> The ZyXEL Device will check whether the incoming phone number is part of any of the groups assigned above before checking which SIP account the call is coming to.
PSTN Call	Select a ring for PSTN calls.
Internal Call	Select a ring for internal calls.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 14

## PSTN Line

This chapter applies to P-2608HWL-Dx models only. Use this screen to set up the PSTN line used to make regular phone calls. These phone calls do not use the Internet.

### 14.1 PSTN Line Overview

With the Public Switched Telephone Network (PSTN) line, you can make and receive regular phone calls. Use a prefix number to make a regular call. When the ZyXEL Device does not have power, you can make regular calls without dialing a prefix number.

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

**Note:** When the ZyXEL Device does not have power, only the phone connected to the **PHONE 1** port can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.

### 14.2 PSTN Line Screen

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

**Figure 99** VoIP > PSTN Line > General

The screenshot shows a web interface for configuring a PSTN line. At the top, there is a tab labeled 'General'. Below it, the section is titled 'Call through PSTN Line'. There is a text input field for 'PSTN Line Pre-fix Number' containing the value '0000'. Below this is a section for 'Relay to PSTN Line' with nine numbered input fields (1 through 9). At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

Each field is described in the following table.

**Table 67** VoIP > PSTN Line > General

LABEL	DESCRIPTION
PSTN Line Pre-fix Number	Enter 1 - 7 telephone keys (0 - 9, #, *) you dial before you dial the phone number, if you want to make a regular phone call while one of your SIP accounts is registered. These numbers tell the ZyXEL Device that you want to make a regular phone call. It is not recommended to use the # key, however, because it is also used in <b>Immediate Dial</b> . (See <b>VoIP &gt; Phone &gt; Common</b> .)
Relay to PSTN Line	Enter phone numbers (for regular calls, not VoIP calls) that you want to dial without the prefix number. For example, you should enter emergency numbers. The number (1 - 9) is not a speed-dial number. It is just a sequential value that is not associated with any phone number.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

# CHAPTER 15

## Firewalls

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

### 15.1 Firewall Overview

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

Refer to [Section 16.5 on page 202](#) to configure default firewall settings.

Refer to [Section 16.6 on page 203](#) to view firewall rules.

Refer to [Section 16.6.1 on page 205](#) to configure firewall rules.

Refer to [Section 16.6.2 on page 208](#) to configure a custom service.

Refer to [Section 16.8.3 on page 215](#) to configure firewall thresholds.

### 15.2 Types of Firewalls

There are three main types of firewalls:

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

#### 15.2.1 Packet Filtering Firewalls

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

## 15.2.2 Application-level Firewalls

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

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

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

## 15.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See [Section 15.5 on page 193](#) for more information on stateful inspection.

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

## 15.3 Introduction to ZyXEL's Firewall

The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The ZyXEL Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyXEL Device also has packet filtering capabilities.

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

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

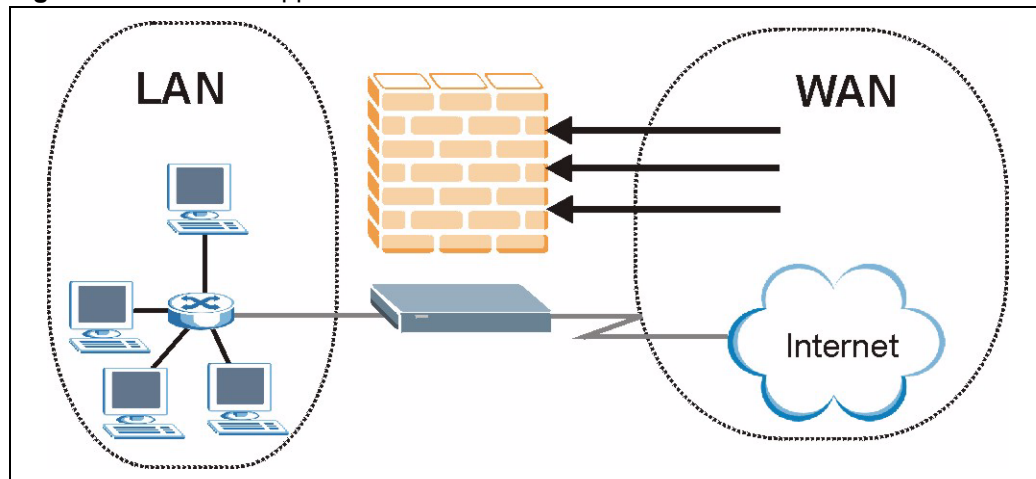
- The DSL/ISDN port connects to the Internet.



- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, “inbound access” will not be allowed unless you configure remote management or create a firewall rule to allow a remote host to use a specific service.

### 15.3.1 Denial of Service Attacks

Figure 100 Firewall Application



## 15.4 Denial of Service

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

### 15.4.1 Basics

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

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

Some of the most common IP ports are:

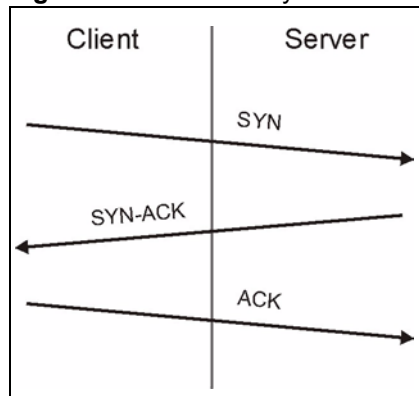
**Table 68** Common IP Ports

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

## 15.4.2 Types of DoS Attacks

There are four types of DoS attacks:

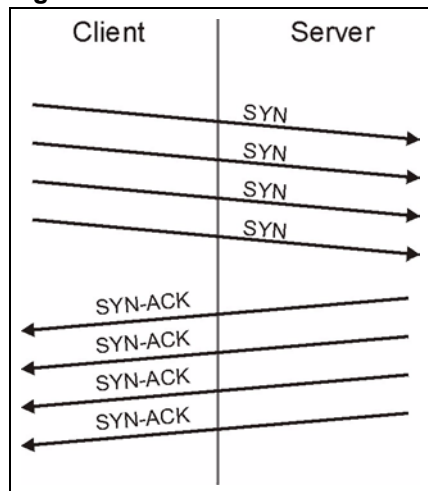
- 1 Those that exploit bugs in a TCP/IP implementation.
- 2 Those that exploit weaknesses in the TCP/IP specification.
- 3 Brute-force attacks that flood a network with useless data.
- 4 IP Spoofing.
- 5 **"Ping of Death"** and **"Teardrop"** attacks exploit bugs in the TCP/IP implementations of various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

**Figure 101** Three-Way Handshake

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

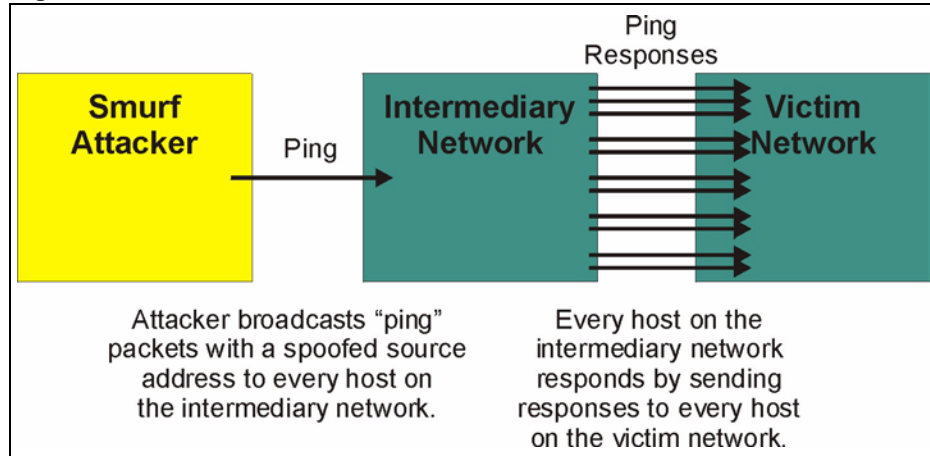
- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs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

**Figure 102** SYN Flood



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

**Figure 103** Smurf Attack



### 15.4.2.1 ICMP Vulnerability

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

**Table 69** ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

### 15.4.2.2 Illegal Commands (NetBIOS and SMTP)

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

**Table 70** Legal NetBIOS Commands

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

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

**Table 71** Legal SMTP Commands

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

### 15.4.2.3 Traceroute

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

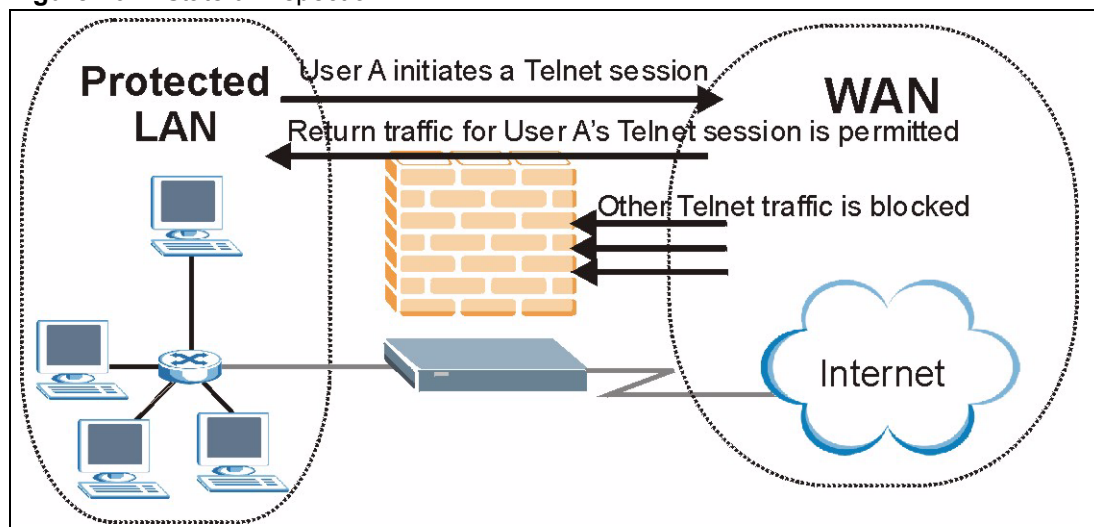
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking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

## 15.5 Stateful Inspection

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

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

**Figure 104** Stateful Inspection



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

### 15.5.1 Stateful Inspection Process

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

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

### 15.5.2 Stateful Inspection on Your ZyXEL Device

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

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

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

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

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

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

### 15.5.3 TCP Security

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

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

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

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

### 15.5.4 UDP/ICMP Security

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

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

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

### 15.5.5 Upper Layer Protocols

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

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

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

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

## 15.6 Guidelines for Enhancing Security with Your Firewall

- Change the default password.
- Limit who can telnet into your router.
- Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- Protect against IP spoofing by making sure the firewall is active.
- Keep the firewall in a secured (locked) room.

### 15.6.1 Security In General

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



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

## 15.7 Packet Filtering Vs Firewall

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

### 15.7.1 Packet Filtering:

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

### 15.7.1.1 When To Use Filtering

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

### 15.7.2 Firewall

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

#### 15.7.2.1 When To Use The Firewall

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

# CHAPTER 16

## Firewall Configuration

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

### 16.1 Access Methods

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

### 16.2 Firewall Policies Overview

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

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

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

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

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

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

- WAN to LAN
- WAN to WAN/ Router

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

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

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

For example, you may create rules to:

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

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

## 16.3 Rule Logic Overview

**Note:** Study these points carefully before configuring rules.

### 16.3.1 Rule Checklist

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

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

### 16.3.2 Security Ramifications

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

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

### 16.3.3 Key Fields For Configuring Rules

#### 16.3.3.1 Action

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

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

#### 16.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See [Appendix D on page 387](#) for more information on predefined services.

#### 16.3.3.3 Source Address

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

#### 16.3.3.4 Destination Address

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

## 16.4 Connection Direction

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

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

## 16.4.1 LAN to WAN Rules

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

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

## 16.4.2 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when a rule is matched in the **Edit Rule** screen (see [Figure 107 on page 206](#)). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen. Refer to [Chapter 26 on page 325](#) for details.

## 16.5 General Firewall Policy

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

Refer to [Section 15.1 on page 187](#) for more information.

**Figure 105** Firewall: General

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

The following table describes the labels in this screen.

**Table 72** Firewall: General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	<p>Select this check box to have the ZyXEL Device firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology.</p> <p><b>Note:</b> Allowing asymmetrical routes may let traffic from the WAN go directly to a LAN computer without passing through the router. See <a href="#">Appendix F on page 399</a> for more on triangle route topology and how to deal with this problem.</p>
Packet Direction	<p>This is the direction of travel of packets (<b>LAN to LAN / Router, LAN to WAN, WAN to WAN / Router, WAN to LAN</b>).</p> <p>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, <b>LAN to LAN / Router</b> means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyXEL Device or the ZyXEL Device itself.</p>
Default Action	<p>Use the drop-down list boxes to select the default action that the firewall is take on packets that are traveling in the selected direction and do not match any of the firewall rules.</p> <p>Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select <b>Permit</b> to allow the passage of the packets.</p>
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this button to display more information.
Basic...	Click this button to display less information.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 16.6 Firewall Rules Summary

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

Refer to [Section 15.1 on page 187](#) for more information.

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

**Figure 106** Firewall Rules

The following table describes the labels in this screen.

**Table 73** 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 <b>Add</b> to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the <b>General</b> screen.	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall rule is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
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 <b>Any</b> .
Service	This drop-down list box displays the services to which this firewall rule applies. See <a href="#">Appendix D on page 387</a> for more information.
Action	This field displays whether the firewall silently discards packets ( <b>Drop</b> ), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender ( <b>Reject</b> ) or allows the passage of packets ( <b>Permit</b> ).
Schedule	This field tells you whether a schedule is specified ( <b>Yes</b> ) or not ( <b>No</b> ).
Log	This field shows you whether a log is created when packets match this rule ( <b>Yes</b> ) or not ( <b>No</b> ).



**Table 73** 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 <b>Move the rule to</b> field. Type a number in the <b>Move the rule to</b> field and click the <b>Move</b> 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 <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

### 16.6.1 Configuring Firewall Rules

Refer to [Section 15.1 on page 187](#) for more information.

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

**Figure 107** Firewall: Edit Rule

**Edit Rule 2**

Active  
 Action for Matched Packets: Permit ▼

---

**Source Address**

Address Type: Any Address ▼

Start IP Address:        

End IP Address:        

Subnet Mask:        

---

**Destination Address**

Address Type: Any Address ▼

Start IP Address:        

End IP Address:        

Subnet Mask:        

---

**Service**

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

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

[Edit Customized Services](#)

---

**Schedule**

Day to Apply

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

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

All day

Start  hour  minute    End  hour  minute

Log

Log Packet Detail Information.

Alert

Send Alert Message to Administrator When Matched.

-----

The following table describes the labels in this screen.

**Table 74** Firewall: Edit Rule

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select <b>Reject</b> 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 <b>Permit</b> 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: <b>Single Address</b> , <b>Range Address</b> , <b>Subnet Address</b> and <b>Any Address</b> .
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 <b>Add &gt;&gt;</b> to add a new address to the <b>Source</b> or <b>Destination Address</b> 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 <b>Edit &lt;&lt;</b> .
Delete	Highlight an existing source or destination address from the <b>Source</b> or <b>Destination Address</b> box above and click <b>Delete</b> to remove it.
Service	
Available/ Selected Services	Please see <a href="#">Appendix D on page 387</a> for more information on services available. Highlight a service from the <b>Available Services</b> box on the left, then click <b>Add &gt;&gt;</b> to add it to the <b>Selected Services</b> box on the right. To remove a service, highlight it in the <b>Selected Services</b> box on the right, then click <b>Remove</b> .
Edit Customized Service	Click the <b>Edit Customized Services</b> 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 <b>All Day</b> 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 <b>Log Settings</b> page and select the <b>Access Control</b> logs category to have the ZyXEL Device record these logs.
Alert	
Send Alert Message to Administrator When Matched	Select the check box to have the ZyXEL Device generate an alert when the rule is matched.
Back	Click <b>Back</b> to return to the previous screen.

**Table 74** Firewall: Edit Rule (continued)

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

## 16.6.2 Customized Services

Configure customized services and port numbers not predefined by the ZyXEL Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix D on page 387](#) for some examples. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Refer to [Section 15.1 on page 187](#) for more information.

**Figure 108** Firewall: Customized Services

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

Back

The following table describes the labels in this screen.

**Table 75** Customized Services

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

### 16.6.3 Configuring A Customized Service

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

Refer to [Section 15.1 on page 187](#) for more information.

**Figure 109** Firewall: Configure Customized Services

The following table describes the labels in this screen.

**Table 76** Firewall: Configure Customized Services

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port ( <b>TCP</b> , <b>UDP</b> or <b>TCP/UDP</b> ) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click <b>Single</b> to specify one port only or <b>Port Range</b> to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click <b>Back</b> to return to the previous screen without saving your changes.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.
Delete	Click <b>Delete</b> to delete the current rule.

## 16.7 Example Firewall Rule

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

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

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

**Figure 110** Firewall Example: Rules

General **Rules** Threshold

Rules

Firewall Rules Storage Space in Use ( 3%)

0% 100%

Packet Direction WAN to LAN

Create a new rule after rule number : 0 Add

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

Apply Cancel

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

**Figure 111** Edit Custom Port Example

Config

Service Name MyService

Service Type TCP/UDP

Port Configuration

Type  Single  Port Range

Port Number From 123 To 123

Back Apply Cancel Delete

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

**Figure 112** Firewall Example: Edit Rule: Destination Address

Edit Rule 1	
<input checked="" type="checkbox"/> Active	Action for Matched Packets: <b>Permit</b> ▼
Source Address	
Address Type: <b>Any Address</b> ▼	Source Address List
Start IP Address: 0.0.0.0	<input type="button" value="Add &gt;&gt;"/> <input type="button" value="Edit &lt;&lt;"/> <input type="button" value="Delete"/>
End IP Address: 0.0.0.0	
Subnet Mask: 0.0.0.0	
	<div style="border: 1px solid gray; padding: 2px;">Any</div>
Destination Address	
Address Type: <b>Range Address</b> ▼	Destination Address List
Start IP Address: 10.0.0.10	<input type="button" value="Add &gt;&gt;"/> <input type="button" value="Edit &lt;&lt;"/> <input type="button" value="Delete"/>
End IP Address: 10.0.0.15	
Subnet Mask: 0.0.0.0	
	<div style="border: 1px solid gray; padding: 2px;">10.0.0.10 - 10.0.0.15</div>
Service	

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

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

**Figure 113** Firewall Example: Edit Rule: Select Customized Services

**Edit Rule 2**

Active  
 Action for Matched Packets: Permit

**Source Address**

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Add >>

Edit <<

Delete

Source Address List

Any

**Destination Address**

Address Type: Range Address

Start IP Address: 10.0.0.10

End IP Address: 10.0.0.15

Subnet Mask: 0.0.0.0

Add >>

Edit <<

Delete

Destination Address List

10.0.0.10 - 10.0.0.15

**Service**

Available Services

Any(All)

Any(ICMP)

AIMNEW-ICQ(TCP:5190)

AUTH(TCP:113)

BGP(TCP:179)

[Edit Customized Services](#)

Add >>

Remove

Selected Services

\*MyService(TCP/UDP:123)

**Schedule**

Day to Apply

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

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

All day

Start  hour  minute    End  hour  minute

Log

Log Packet Detail Information.

Alert

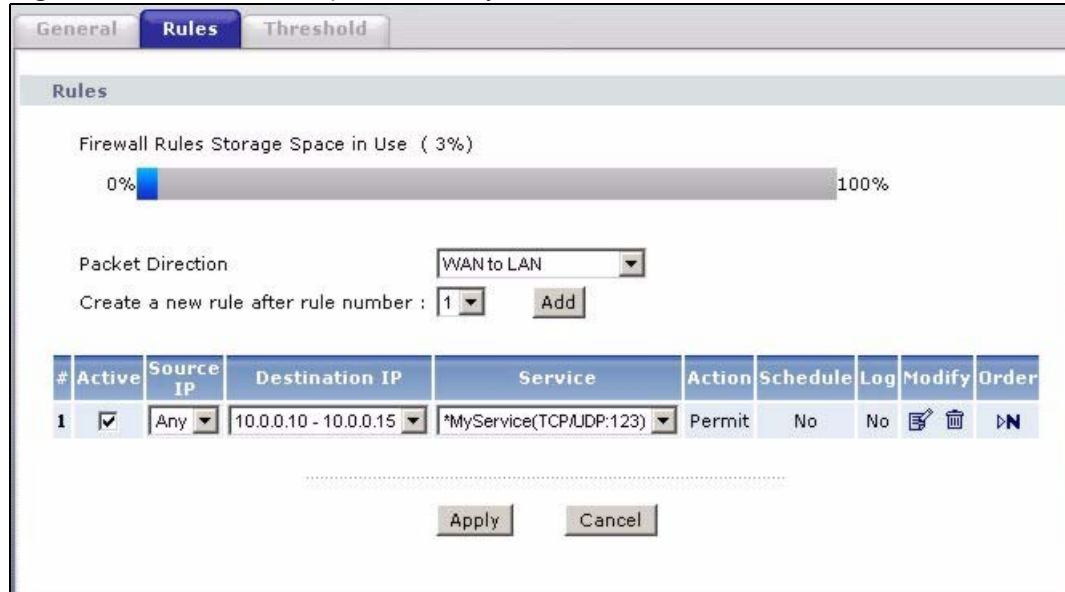
Send Alert Message to Administrator When Matched.

Back    **Apply**    Cancel

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

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



**Figure 114** Firewall Example: Rules: MyService

## 16.8 DoS Thresholds

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

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

Refer to [Section 16.8.3 on page 215](#) to configure thresholds.

### 16.8.1 Threshold Values

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

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

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

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

## 16.8.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see [Figure 101 on page 190](#)). 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.

### 16.8.2.1 TCP Maximum Incomplete and Blocking Time

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

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

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

### 16.8.3 Configuring Firewall Thresholds

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

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

**Figure 115** Firewall: Threshold

The following table describes the labels in this screen.

**Table 77** Firewall: Threshold

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

**Table 77** Firewall: Threshold (continued)

LABEL	DESCRIPTION	DEFAULT VALUES
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set <b>Maximum Incomplete High</b> to lower than the current <b>Maximum Incomplete Low</b> number.	100 existing half-open sessions. The above values causes the ZyXEL Device to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10 existing half-open TCP sessions.
Action taken when the TCP Maximum Incomplete reached threshold		
Delete the Oldest Half Open Session when New Connection Request Comes.	Select this radio button to clear the oldest half open session when a new connection request comes.	
Deny New Connection Request for	Select this radio button and specify for how long the ZyXEL Device should block new connection requests when <b>TCP Maximum Incomplete</b> is reached. Enter the length of blocking time in minutes (between 1 and 256).	
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.	
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.	

# CHAPTER 17

## Content Filtering

This chapter covers how to configure content filtering.

### 17.1 Content Filtering Overview

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

### 17.2 Configuring Keyword Blocking

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

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

**Figure 116** Content Filter: Keyword

The screenshot shows the 'Content Filter: Keyword' configuration window. It features three tabs: 'Keyword' (active), 'Schedule', and 'Trusted'. The 'Keyword' tab contains a section titled 'Keyword' with a checked checkbox for 'Active Keyword Blocking'. Below this is a text area labeled 'Block Websites that contain these keywords in the URL :' containing the word 'bad'. There are 'Delete' and 'Clear All' buttons below the text area. At the bottom, there is a 'Keyword' input field and an 'Add Keyword' button. At the very bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 78** Content Filter: Keyword

LABEL	DESCRIPTION
Active Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the ZyXEL Device to block.
Delete	Highlight a keyword in the box and click <b>Delete</b> to remove it.
Clear All	Click <b>Clear All</b> to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click <b>Add Keyword</b> after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 17.3 Configuring the Schedule

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

**Figure 117** Content Filter: Schedule

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

The following table describes the labels in this screen.

**Table 79** Content Filter: Schedule

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

## 17.4 Configuring Trusted Computers

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

**Figure 118** Content Filter: Trusted

The following table describes the labels in this screen.

**Table 80** Content Filter: Trusted

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





# CHAPTER 18

## IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the ZyXEL Device.

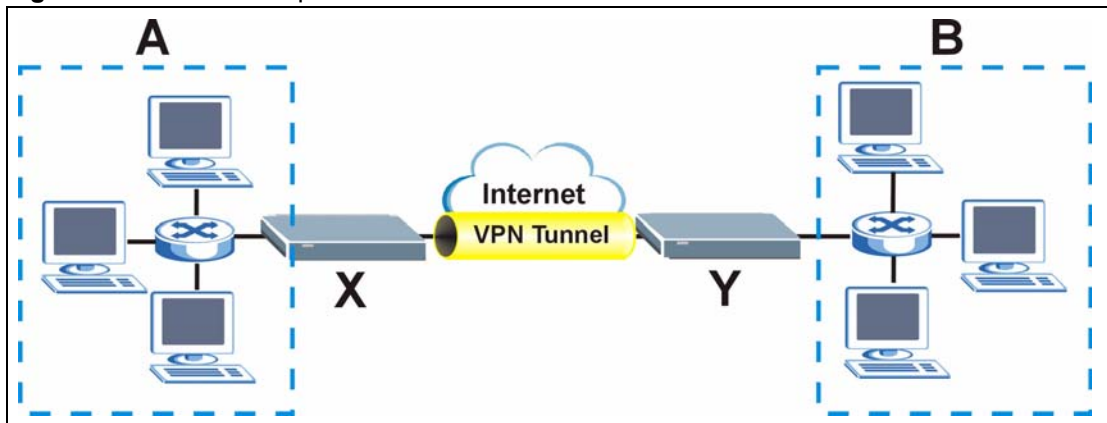
### 18.1 IPSec VPN Overview

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

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

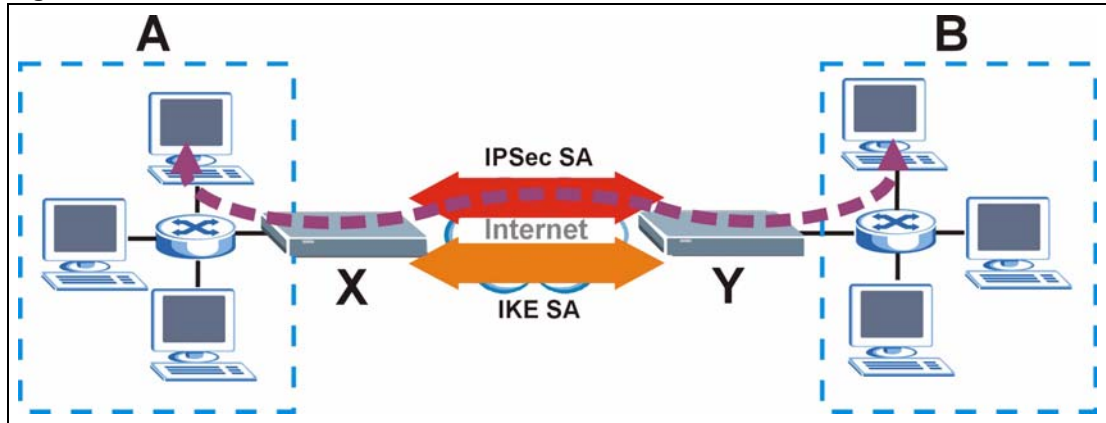
The following figure is one example of a VPN tunnel.

**Figure 119** VPN: Example



The VPN tunnel connects the ZyXEL Device (X) and the remote IPsec router (Y). These routers then connect the local network (A) and remote network (B).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyXEL Device and the remote IPsec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyXEL Device and remote IPsec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyXEL Device and remote IPsec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

**Figure 120** VPN: IKE SA and IPsec SA

In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by the tunneling, encryption, and authentication of the IPsec SA. The IPsec SA is established securely using the IKE SA that routers **X** and **Y** established first.

The rest of this section discusses IKE SA and IPsec SA in more detail.

### 18.1.1 IKE SA Overview

The IKE SA provides a secure connection between the ZyXEL Device and remote IPsec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many steps are required. There are two negotiation modes: main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

**Note:** Both routers must use the same negotiation mode.

These modes are discussed in more detail in [Section 18.1.2.1 on page 226](#). The examples in this section use main mode.

#### 18.1.1.1 IP Addresses of the ZyXEL Device and Remote IPsec Router

In the ZyXEL Device, you have to specify the IP addresses of the ZyXEL Device and the remote IPsec router to establish an IKE SA.

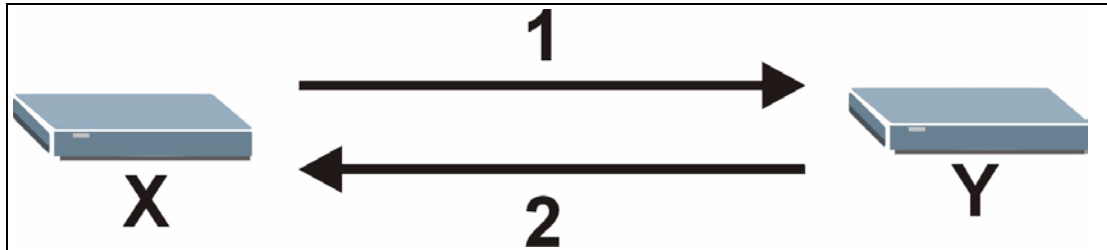
You can usually provide a static IP address or a domain name for the ZyXEL Device. Sometimes, your ZyXEL Device might also offer another alternative, such as using the IP address of a port or interface.

You can usually provide a static IP address or a domain name for the remote IPsec router as well. Sometimes, you might not know the IP address of the remote IPsec router (for example, telecommuters). In this case, you can still set up the IKE SA, but only the remote IPsec router can initiate an IKE SA.

### 18.1.1.2 IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the ZyXEL Device and remote IPsec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated below.

**Figure 121** IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The ZyXEL Device sends one or more proposals to the remote IPsec router. (In some devices, you can set up only one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the ZyXEL Device wants to use in the IKE SA. The remote IPsec router selects an acceptable proposal and sends the accepted proposal back to the ZyXEL Device. If the remote IPsec router rejects all of the proposals (for example, if the VPN tunnel is not configured correctly), the ZyXEL Device and remote IPsec router cannot establish an IKE SA.

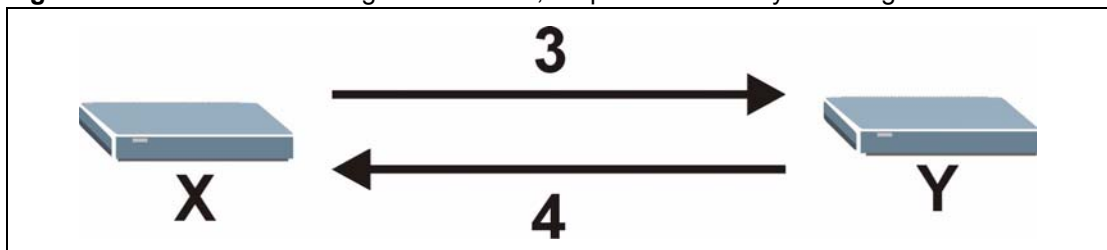
**Note:** Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

See the field descriptions for information about specific encryption algorithms, authentication algorithms, and DH key groups. You can also see [Section 18.1.1.3 on page 223](#) for more information about the role of DH key groups.

### 18.1.1.3 Diffie-Hellman (DH) Key Exchange

The ZyXEL Device and the remote IPsec router use a DH key exchange to establish a shared secret, which is used to generate encryption keys for IKE SA and IPsec SA. In main mode, the DH key exchange is done in steps 3 and 4, as illustrated below.

**Figure 122** IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



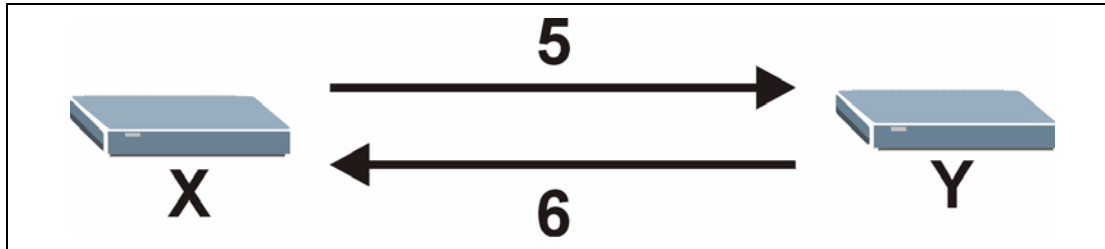
The DH key exchange is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption keys, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 encryption keys take longer to encrypt and decrypt.

### 18.1.1.4 Authentication

Before the ZyXEL Device and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the ZyXEL Device and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. Their identities are encrypted using the encryption algorithm and encryption key the ZyXEL Device and remote IPSec router selected in previous steps.

**Figure 123** IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication



The ZyXEL Device and remote IPSec router use a pre-shared key in the authentication process, though it is not actually transmitted or exchanged.

**Note:** The ZyXEL Device and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and ID content. The ID type can be IP address, domain name, or e-mail address, and the ID content is a specific IP address, domain name, or e-mail address. The ID content is only used for identification; the IP address, domain name, or e-mail address that you enter does not have to actually exist.

The ZyXEL Device and the remote IPSec router each has its own identity, so each one must store two sets of information, one for itself and one for the other router. Local ID type and ID content refers to the ID type and ID content that applies to the router itself, and peer ID type and ID content refers to the ID type and ID content that applies to the other router in the IKE SA.

**Note:** The ZyXEL Device's local and peer ID type and ID content must match the remote IPSec router's peer and local ID type and ID content, respectively.

In the following example, the ZyXEL Device and the remote IPSec router authenticate each other successfully.

**Table 81** VPN Example: Matching ID Type and Content

ZYXEL DEVICE	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

In the following example, the authentication fails, so they cannot establish an IKE SA.

**Table 82** VPN Example: Mismatching ID Type and Content

ZYXEL DEVICE	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: <b>1.1.1.2</b>
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: <b>1.1.1.15</b>	Peer ID content: tom@yourcompany.com

It is also possible to configure the ZyXEL Device to ignore the identity of the remote IPsec router. In this case, you usually set the peer ID type to **Any**. This is not as secure as other peer ID types, however.

#### 18.1.1.4.1 Certificates

It is also possible for the ZyXEL Device and remote IPsec router to authenticate each other with certificates. In this case, the authentication process is different.

- Instead of using the pre-shared key, the ZyXEL Device and remote IPsec router check each other's certificates.
- The local ID type and ID content come from the certificate. On the ZyXEL Device, you simply select which certificate to use.
- If you set the peer ID type to **Any**, the ZyXEL Device authenticates the remote IPsec router using the trusted certificates and trusted CAs you have set up. Alternatively, if you want to use a specific certificate to authenticate the remote IPsec router, you can use the information in the certificate to specify the peer ID type and ID content.

**Note:** You must set up the certificates for the ZyXEL Device and remote IPsec router before you can use certificates in IKE SA. See [Chapter 19 on page 249](#) for more information about certificates.

#### 18.1.1.5 Extended Authentication

Extended authentication is often used when multiple IPsec routers use the same VPN tunnel to connect to a single IPsec router. For example, this might be used with telecommuters. Extended authentication occurs right after the authentication described in [Section 18.1.1.4 on page 224](#).

In extended authentication, one of the routers (the ZyXEL Device or the remote IPsec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the ZyXEL Device to provide a user name and password to the remote IPsec router, or you can set up the ZyXEL Device to check a user name and password that is provided by the remote IPsec router.

## 18.1.2 Additional Topics for IKE SA

This section provides more information about IKE SA.

### 18.1.2.1 Negotiation Mode

There are two negotiation modes: main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1-2: The ZyXEL Device sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the ZyXEL Device.

Steps 3-4: The ZyXEL Device and the remote IPSec router participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

Steps 5-6: Finally, the ZyXEL Device and the remote IPSec router generate an encryption key from the shared secret, encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA.

Step 1: The ZyXEL Device sends its proposals to the remote IPSec router. It also starts the Diffie-Hellman key exchange and sends its (unencrypted) identity to the remote IPSec router for authentication.

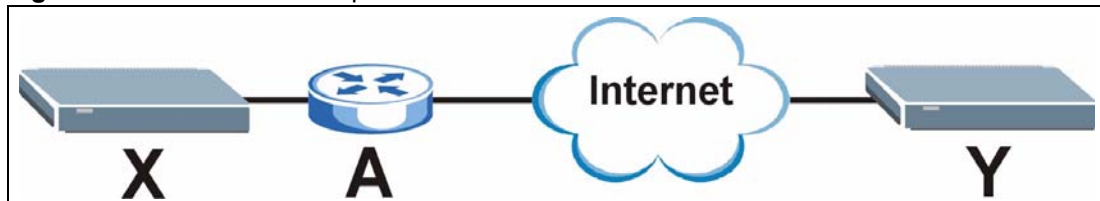
Step 2: The remote IPSec router selects an acceptable proposal and sends it back to the ZyXEL Device. It also finishes the Diffie-Hellman key exchange, authenticates the ZyXEL Device, and sends its (unencrypted) identity to the ZyXEL Device for authentication.

Step 3: The ZyXEL Device authenticates the remote IPSec router and confirms that the IKE SA is established.

Aggressive mode does not provide as much security as main mode because the identity of the ZyXEL Device and the identity of the remote IPSec router are not encrypted. It is usually used when the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication (for example, telecommuters).

### 18.1.2.2 VPN, NAT and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

**Figure 124** VPN/NAT Example

If router **A** does NAT, it might change IP addresses (source or destination), port numbers (source or destination), or any combination of these. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because authentication depends on the original IP addresses and port numbers.

Most routers that support NAT (like router **A**) have an IPSec pass-through feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See [Section 18.1.3.2 on page 228](#) for more information about active protocols.)

If router **A** does not have an IPSec pass-through or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the ZyXEL Device and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the ZyXEL Device and remote IPSec router support.

**Note:** You must enable NAT traversal on the ZyXEL Device and the remote IPSec router, and you must configure the NAT router to forward packets with the extra header unchanged.

### 18.1.3 IPSec SA Overview

Once the ZyXEL Device and remote IPSec router have established the IKE SA, they can use the IKE SA to securely negotiate IPSec SAs through which to send data between computers on the networks.

**Note:** An IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of IPSec SA.

### 18.1.3.1 Local Network and Remote Network

In IPsec SA terminology, the local network, the one(s) connected to the ZyXEL Device, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPsec router, may be called the remote policy.

### 18.1.3.2 Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPsec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

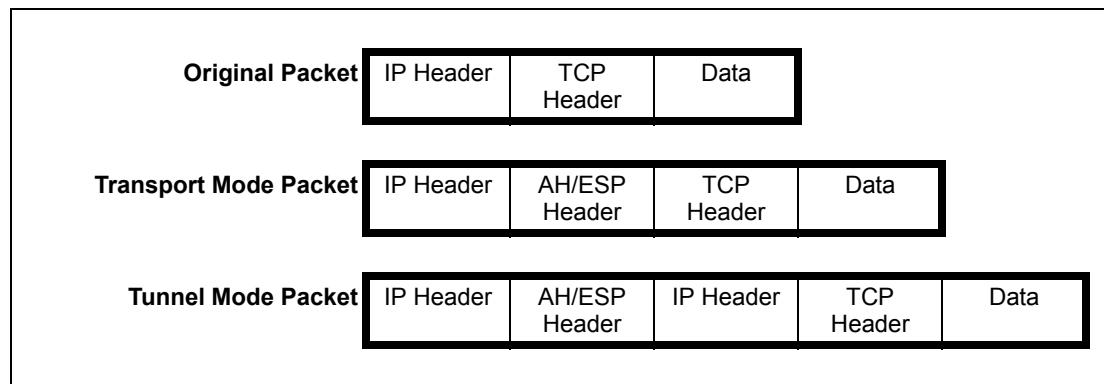
**Note:** The ZyXEL Device and remote IPsec router must use the same active protocol. ESP is recommended.

ESP is recommended because AH does not support encryption and ESP is more suitable with NAT. Use AH only if the remote IPsec router does not support ESP.

### 18.1.3.3 Encapsulation

There are two ways to encapsulate packets. These modes are illustrated below.

**Figure 125** VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the ZyXEL Device encapsulates the entire IP packet. As a result, there are two IP headers, as well as the header for the active protocol.

- Outside header: The outside IP header contains the IP addresses of the ZyXEL Device and remote IPsec router.
- AH/ESP header: The header for the active protocol encapsulates the original packet.
- Inside header: The inside IP header contains the IP address of the computers behind the ZyXEL Device or remote IPsec router.



In transport mode, the IP header is the original IP header, and the encapsulation depends on the active protocol. If the active protocol is AH, the ZyXEL Device includes part of the IP header when it encapsulates the packet. If the active protocol is ESP, the ZyXEL Device does not include the original IP header when it encapsulates the packet, in which case it is not possible to verify the integrity of the source IP address.

**Note:** The ZyXEL Device and remote IPSec router must use the same encapsulation.

Usually, you should use tunnel mode because it is more secure. Transport mode should only be used when the IPSec SA is used for communication between the ZyXEL Device and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

#### 18.1.3.4 IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see [Section 18.1.1.2 on page 223](#)), except that you also have the choice whether or not the ZyXEL Device and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the ZyXEL Device and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the shared secret from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys are secure because they are created from different shared secrets.

If you do not enable PFS, the ZyXEL Device and remote IPSec router use the same shared secret that was generated when the IKE SA was established to generate encryption keys. The ZyXEL Device and remote IPSec router still create a new shared secret every time they establish (or re-establish) the IKE SA.

A DH key exchange is time-consuming. You might consider disabling PFS, if it takes a long time to establish IPSec SA and if the VPN tunnel has good security (for example, strong encryption) without it.

### 18.1.4 Additional Topics for IPSec SA

This section provides more information about IPSec SA.

#### 18.1.4.1 IPSec SA using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly (for example, while troubleshooting). You should do this only as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the ZyXEL Device and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SAs and some characteristics of IPSec SAs. There are also some differences between IPSec SAs using manual keys and other types of SAs.

#### 18.1.4.1.1 IPsec SA Proposal using Manual Keys

In IPsec SAs using manual keys, you can only specify one encryption algorithm and one authentication algorithm. You cannot specify several proposals. There is no DH key exchange, so you have to provide the encryption key and the authentication key the ZyXEL Device and remote IPsec router use.

**Note:** The ZyXEL Device and remote IPsec router must use the same encryption key and authentication key.

#### 18.1.4.1.2 Authentication and the Security Parameter Index (SPI)

In IPsec SAs using manual keys, the ZyXEL Device and remote IPsec router use the SPI, instead of pre-shared keys, ID type and ID content, for authentication. The SPI is an arbitrary number that is used to help identify the IPsec SA.

**Note:** The ZyXEL Device and remote IPsec router must use the same SPI.

## 18.2 VPN Setup Screen

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

Figure 126 VPN Setup

The screenshot shows the 'VPN Setup' configuration page. At the top, there are three tabs: 'Setup', 'Monitor', and 'VPN Global Setting'. Below the tabs is a 'Summary' section containing a table with 20 rows. Each row represents a VPN policy with columns for 'No.', 'Active', 'Name', 'Local Address', 'Remote Address', 'Encap.', 'IPSec Algorithm', 'Secure Gateway IP', and 'Modify'. The 'Modify' column contains edit and delete icons. Below the table are 'Apply' and 'Cancel' buttons.

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

The following table describes the fields in this screen.

Table 83 VPN Setup

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

**Table 83** VPN Setup

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

## 18.3 Editing VPN Policies

Click an **Edit** icon in the **VPN Setup Screen** to edit VPN policies.

**Figure 127** Edit VPN Policies

The screenshot shows the 'Edit VPN Policies' configuration interface. It is organized into five main sections:

- IPSec Setup:** Includes checkboxes for 'Active', 'Keep Alive', and 'NAT Traversal'. Fields for 'Name', 'IPSec Key Mode' (set to IKE), 'Negotiation Mode' (set to Main), 'Encapsulation Mode' (set to Tunnel), and 'DNS Server (for IPsec VPN)' (set to 0.0.0.0).
- Local:** Fields for 'Local Address Type' (Single), 'IP Address Start' (0.0.0.0), and 'End / Subnet Mask' (0.0.0.0).
- Remote:** Fields for 'Remote Address Type' (Single), 'IP Address Start' (0.0.0.0), and 'End / Subnet Mask' (0.0.0.0).
- Address Information:** Fields for 'Local ID Type' (IP), 'Content', 'My IP Address' (0.0.0.0), 'Peer ID Type' (IP), 'Content', and 'Secure Gateway Address' (0.0.0.0).
- Security Protocol:** Fields for 'VPN Protocol' (ESP), 'Pre-Shared Key', 'Encryption Algorithm' (AES), and 'Authentication Algorithm' (SHA1).

At the bottom, there are four buttons: 'Back', 'Apply', 'Cancel', and 'Advanced Setup'.

The following table describes the fields in this screen.

**Table 84** Edit VPN Policies

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

**Table 84** Edit VPN Policies

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

**Table 84** Edit VPN Policies

LABEL	DESCRIPTION
Remote	<p>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the <b>Secure Gateway IP Address</b> field is configured to <b>0.0.0.0</b>. In this case only the remote IPSec router can initiate the VPN.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Remote Address Type	Use the drop-down menu to choose <b>Single</b> , <b>Range</b> , or <b>Subnet</b> . Select <b>Single</b> with a single IP address. Select <b>Range</b> for a specific range of IP addresses. Select <b>Subnet</b> to specify IP addresses on a network by their subnet mask.
IP Address Start	When the <b>Remote Address Type</b> field is configured to <b>Single</b> , enter a (static) IP address on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Range</b> , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Subnet</b> , enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the <b>Remote Address Type</b> field is configured to <b>Single</b> , this field is N/A. When the <b>Remote Address Type</b> field is configured to <b>Range</b> , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Subnet</b> , enter a subnet mask on the network behind the remote IPSec router.
Address Information	
Local ID Type	Select <b>IP</b> to identify this ZyXEL Device by its IP address. Select <b>DNS</b> to identify this ZyXEL Device by a domain name. Select <b>E-mail</b> to identify this ZyXEL Device by an e-mail address.
Content	<p>When you select <b>IP</b> in the <b>Local ID Type</b> field, type the IP address of your computer in the local <b>Content</b> field. The ZyXEL Device automatically uses the IP address in the <b>My IP Address</b> field (refer to the <b>My IP Address</b> field description) if you configure the local <b>Content</b> field to <b>0.0.0.0</b> or leave it blank.</p> <p>It is recommended that you type an IP address other than <b>0.0.0.0</b> in the local <b>Content</b> field or use the <b>DNS</b> or <b>E-mail</b> ID type in the following situations.</p> <p>When there is a NAT router between the two IPSec routers.</p> <p>When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.</p> <p>When you select <b>DNS</b> or <b>E-mail</b> in the <b>Local ID Type</b> field, type a domain name or e-mail address by which to identify this ZyXEL Device in the local <b>Content</b> field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.</p>
My IP Address	<p>Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>The following applies if this field is configured as <b>0.0.0.0</b>:</p> <p>The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel.</p> <p>If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See <a href="#">Chapter 7 on page 89</a> for details on dial backup and traffic redirect.</p>

**Table 84** Edit VPN Policies

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



**Table 84** Edit VPN Policies

LABEL	DESCRIPTION
Encryption Algorithm	<p>Select <b>DES</b>, <b>3DES</b>, <b>AES</b> or <b>NULL</b> from the drop-down list box.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on <b>DES</b> that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of <b>AES</b> uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b>.</p> <p>Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b>, you do not enter an encryption key.</p>
Authentication Algorithm	<p>Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b>, but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.</p>
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click <b>Advanced Setup</b> to configure more detailed settings of your IKE key management.

## 18.4 Configuring Advanced IKE Settings

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

**Figure 128** Advanced VPN Policies

The screenshot shows the 'VPN - IKE - Advanced Setup' configuration interface. It is organized into three main sections:

- VPN - IKE - Advanced Setup:** Contains fields for Protocol (0), Enable Replay Detection (NO), Local Start Port (0) and End (0), and Remote Start Port (0) and End (0).
- Phase1:** Contains fields for Negotiation Mode (Main), Pre-Shared Key (text input), Encryption Algorithm (DES), Authentication Algorithm (MD5), SA Life Time (Seconds) (28800), and Key Group (DH1).
- Phase2:** Contains fields for Active Protocol (ESP), Encryption Algorithm (DES), Authentication Algorithm (SHA1), SA Life Time (Seconds) (28800), Encapsulation (Tunnel), and Perfect Forward Secrecy (PFS) (NONE).

At the bottom of the screen, there are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the fields in this screen.

**Table 85** Advanced VPN Policies

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

**Table 85** Advanced VPN Policies

LABEL	DESCRIPTION
Negotiation Mode	Select <b>Main</b> or <b>Aggressive</b> from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Pre-Shared Key	<p>Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.</p> <p>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62-character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself.</p> <p>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.</p>
Encryption Algorithm	<p>Select <b>DES</b>, <b>3DES</b> or <b>AES</b> from the drop-down list box.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on <b>DES</b> that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b>.</p>
Authentication Algorithm	<p>Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b>, but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.</p>
SA Life Time (Seconds)	<p>Define the length of time before an IPSec SA automatically renegotiates in this field. The minimum value is 180 seconds.</p> <p>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p>
Key Group	<p>You must choose a key group for phase 1 IKE setup. <b>DH1</b> (default) refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.</p>
Phase 2	
Active Protocol	Use the drop-down list box to choose from <b>ESP</b> or <b>AH</b> .
Encryption Algorithm	<p>This field is available when you select <b>ESP</b> in the <b>Active Protocol</b> field.</p> <p>Select <b>DES</b>, <b>3DES</b>, <b>AES</b> or <b>NULL</b> from the drop-down list box.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b>.</p> <p>Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b>, you do not enter an encryption key.</p>

**Table 85** Advanced VPN Policies

LABEL	DESCRIPTION
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop-down list box.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled ( <b>NONE</b> ) by default in phase 2 IPsec SA setup. This allows faster IPsec setup, but is not so secure. Choose <b>DH1</b> or <b>DH2</b> from the drop-down list box to enable PFS. <b>DH1</b> refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device and return to the <b>VPN-IKE</b> screen.
Cancel	Click <b>Cancel</b> to clear your changes.

## 18.5 Configuring Manual Key

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

**Figure 129** VPN: Manual Key

The screenshot shows the 'VPN: Manual Key' configuration page. At the top, there are three tabs: 'Setup' (selected), 'Monitor', and 'VPN Global Setting'. Below the tabs, the page is organized into several sections:

- IPSec Setup:** Includes a checkbox for 'Active', a 'Name' field (containing '2488393585'), an 'IPSec Key Mode' dropdown (set to 'Manual'), an 'SPI' field (containing '0'), an 'Encapsulation Mode' dropdown (set to 'Transport'), and a 'DNS Server (for IPSec VPN)' field (containing '0.0.0.0').
- Local:** Includes a 'Local Address Type' dropdown (set to 'Range'), an 'IP Address Start' field, and an 'End / Subnet Mask' field.
- Remote:** Includes a 'Remote Address Type' dropdown (set to 'Range'), an 'IP Address Start' field, and an 'End / Subnet Mask' field.
- Address Information:** Includes a 'My IP Address' field and a 'Secure Gateway Address' field.
- Security Protocol:** Includes an 'IPSec Protocol' dropdown (set to 'ESP'), an 'Encryption Algorithm' dropdown (set to 'DES'), an 'Encapsulation Key' field, an 'Authentication Algorithm' dropdown (set to 'SHA1'), and an 'Authentication Key' field.

At the bottom of the page, there are three buttons: '< Back', 'Apply', and 'Reset'.

The following table describes the fields in this screen.

**Table 86** VPN: Manual Key

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

**Table 86** VPN: Manual Key (continued)

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

**Table 86** VPN: Manual Key (continued)

LABEL	DESCRIPTION
My IP Address	Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as <b>0.0.0.0</b> : The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel. If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See <a href="#">Chapter 7 on page 89</a> for details on dial backup and traffic redirect.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Security Protocol	
IPSec Protocol	Select <b>ESP</b> if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by <b>AH</b> . If you select ESP here, you must select options from the <b>Encryption Algorithm</b> and <b>Authentication Algorithm</b> fields (described next).
Encryption Algorithm	Select <b>DES</b> , <b>3DES</b> or <b>NULL</b> from the drop-down list box. When <b>DES</b> is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The <b>DES</b> encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ) is a variation on <b>DES</b> that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in increased latency and decreased throughput. Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b> , you do not enter an encryption key.
Encapsulation Key (only with ESP)	With <b>DES</b> , type a unique key 8 characters long. With <b>3DES</b> , type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for <b>MD5</b> authentication or 20 characters for <b>SHA-1</b> authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.

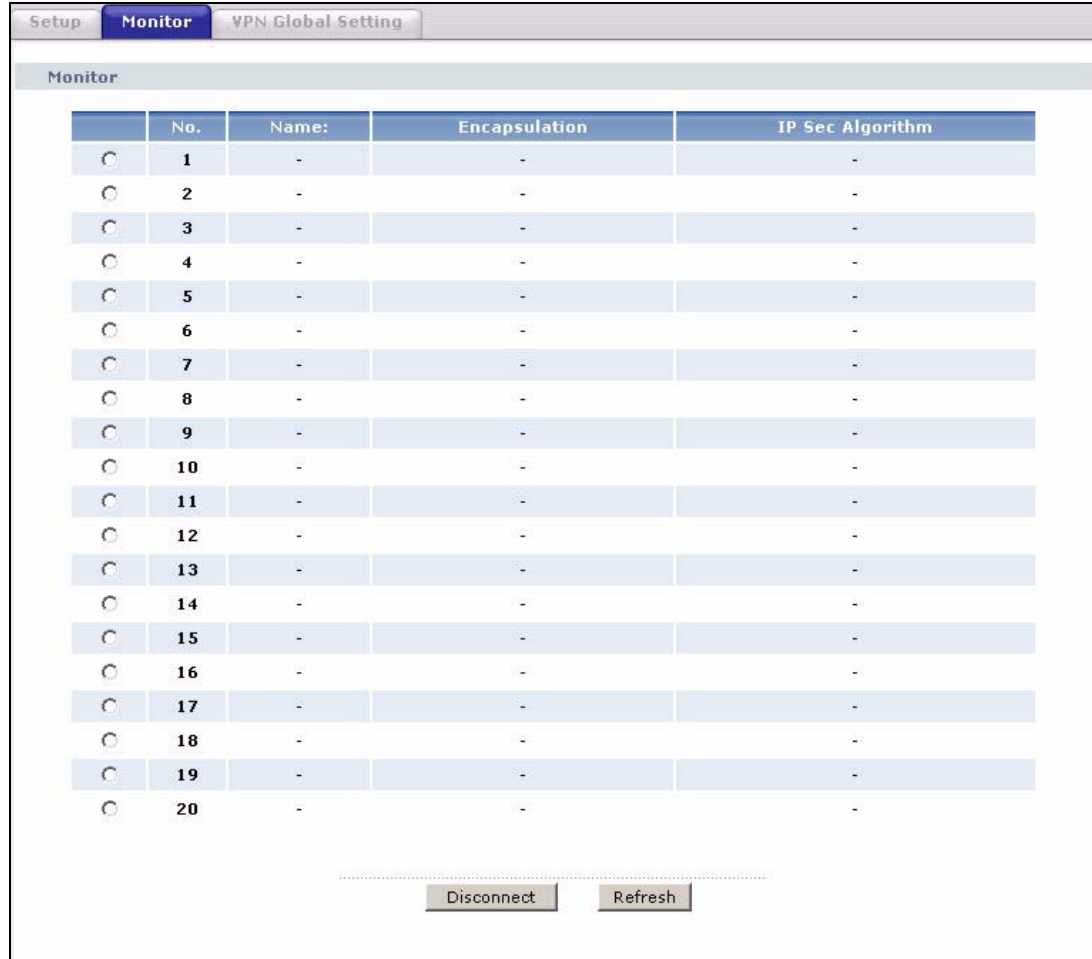
## 18.6 Viewing SA Monitor

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

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

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See [Section 18.1.3 on page 227](#) on keep alive to have the ZyXEL Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

**Figure 130** VPN: SA Monitor



The following table describes the fields in this screen.

**Table 87** VPN: SA Monitor

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



## 18.7 Configuring Global Setting

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

**Figure 131** VPN: Global Setting

The following table describes the fields in this screen.

**Table 88** VPN: Global Setting

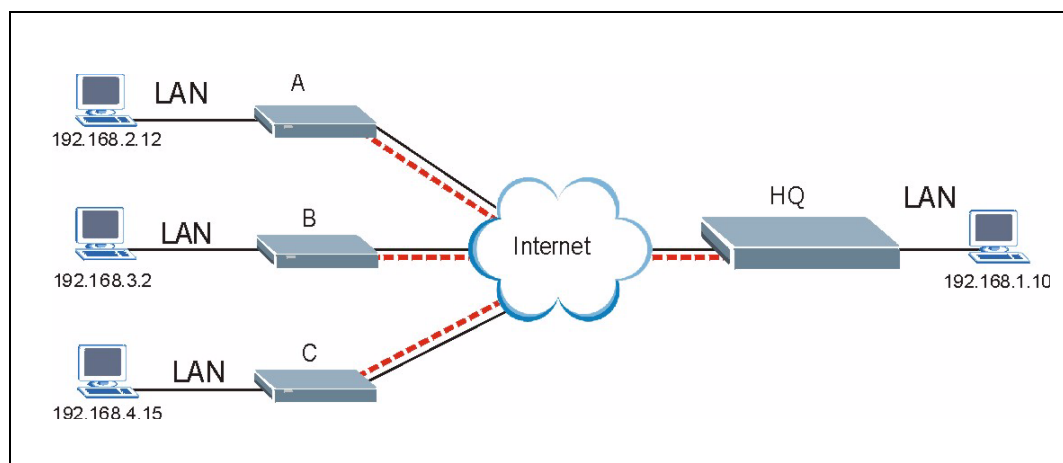
LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers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

## 18.8 Telecommuter VPN/IPSec Examples

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

### 18.8.1 Telecommuters Sharing One VPN Rule Example

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

**Figure 132** Telecommuters Sharing One VPN Rule Example**Table 89** Telecommuters Sharing One VPN Rule Example

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

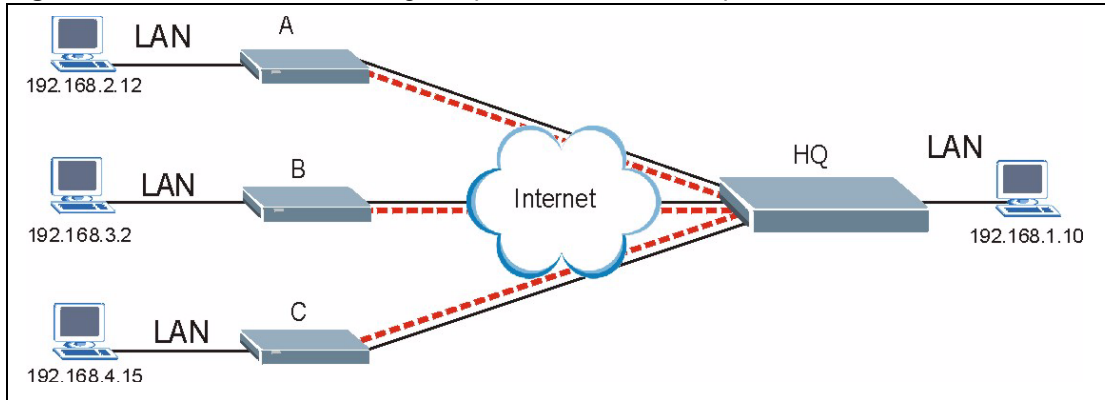
## 18.8.2 Telecommuters Using Unique VPN Rules Example

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

With aggressive negotiation mode (see [Section 18.1.2.1 on page 226](#)), the ZyXEL Device can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyXEL Device at headquarters. They can use different IPsec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyXEL Device at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPsec routers should not overlap.

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

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

**Figure 133** Telecommuters Using Unique VPN Rules Example**Table 90** Telecommuters Using Unique VPN Rules Example

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

## 18.9 VPN and Remote Management

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

# CHAPTER 19

## Certificates

This chapter gives background information about public-key certificates and explains how to use them.

### 19.1 Certificates Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. 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).

### 19.1.1 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.

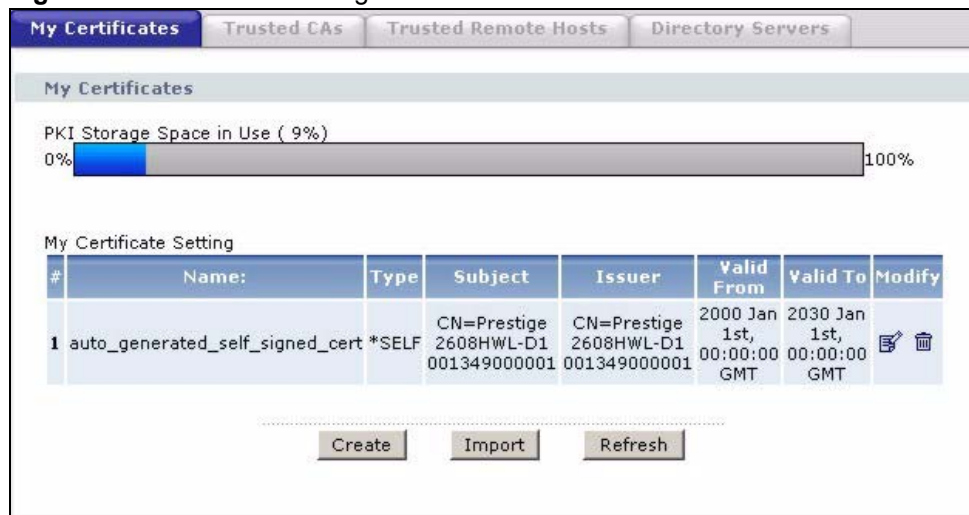
## 19.2 Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the ZyXEL Device act as a certification authority and sign its own certificates.

## 19.3 Configuration Summary

This section summarizes how to manage certificates on the ZyXEL Device.

**Figure 134** Certificate Configuration Overview



Use the **My Certificates** screens to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.

Use the **Trusted CAs** screens to save CA certificates to the ZyXEL Device.

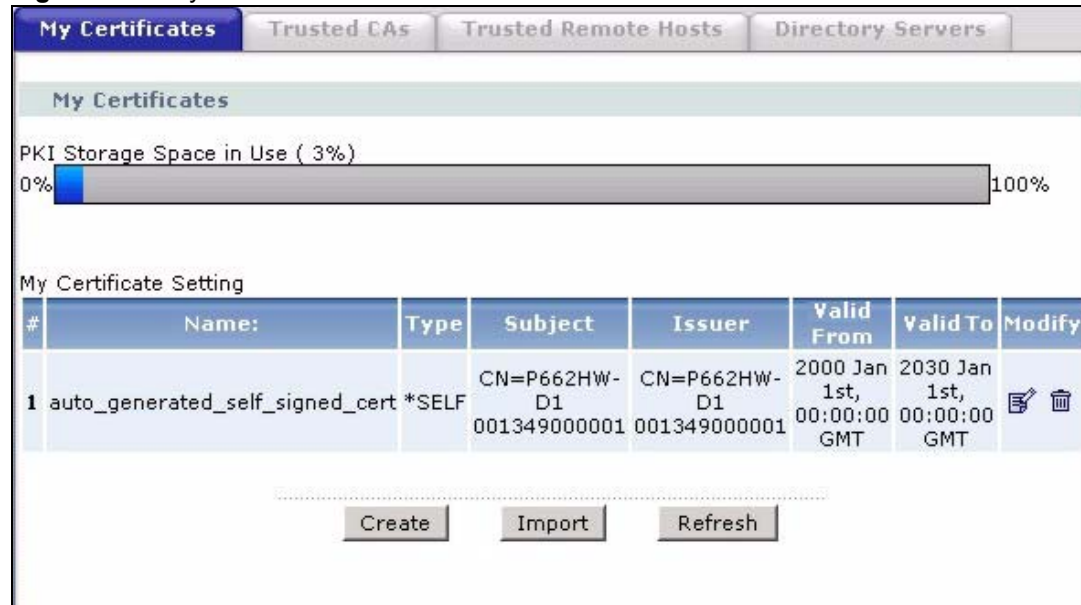
Use the **Trusted Remote Hosts** screens to import self-signed certificates.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

## 19.4 My Certificates

Click **Security > Certificates > My Certificates** to open the **My Certificates** screen. This is the ZyXEL Device's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray.

**Figure 135** My Certificates



The following table describes the labels in this screen.

**Table 91** 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 Devices 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.

**Table 91** My Certificates (continued)

LABEL	DESCRIPTION
#	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	<p>This field displays what kind of certificate this is.</p> <p><b>REQ</b> 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 <b>My Certificate Import</b> screen to import the certificate and replace the request.</p> <p><b>SELF</b> represents a self-signed certificate.</p> <p><b>*SELF</b> represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates.</p> <p><b>CERT</b> represents a certificate issued by a certification authority.</p>
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 <b>Subject</b> 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.
Modify	<p>Click the details icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features is configured to use.</p> <p>Do the following to delete a certificate that shows <b>*SELF</b> in the <b>Type</b> field.</p> <ol style="list-style-type: none"> <li>1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the <b>*SELF</b> certificate.</li> <li>2. Click the details icon next to another self-signed certificate (see the description on the <b>Create</b> button if you need to create a self-signed certificate).</li> <li>3. Select the <b>Default self-signed certificate which signs the imported remote host certificates</b> check box.</li> <li>4. Click <b>Apply</b> to save the changes and return to the <b>My Certificates</b> screen.</li> <li>5. The certificate that originally showed <b>*SELF</b> displays <b>SELF</b> and you can delete it now.</li> </ol> <p>Note that subsequent certificates move up by one when you take this action</p>
Create	Click <b>Create</b> to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.
Import	Click <b>Import</b> 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.
Refresh	Click <b>Refresh</b> to display the current validity status of the certificates.



## 19.5 My Certificate Import

Click **Security > Certificates > My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyXEL Device.

**Note:** You can only import a certificate that matches a corresponding certification request that was generated by the ZyXEL Device.

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.

### 19.5.1 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- 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.

**Figure 136** My Certificate Import

**Certificates - MY Certificates - 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 92** My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the certificate on the ZyXEL Device.
Cancel	Click <b>Cancel</b> to clear your settings.

## 19.6 My Certificate Create

Click **Security > Certificates > My Certificates > Create** to open the **My Certificate Create** 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.

**Figure 137** My Certificate Create

**Certificate Name**

**Subject Information**

Common Name

Host IP Address

Host Domain Name

E-Mail

Organizational Unit

Organization

Country

Key Length  bits

**Enrollment Options**

Create a self-signed certificate

Create a certification request and save it locally for later manual enrollment

Create a certification request and enroll for a certificate immediately online

Enrollment Protocol

CA Server Address

CA Certificate  (See [Trusted CAs](#))

Request Authentication Key

-----

The following table describes the labels in this screen.

**Table 93** My Certificate 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 <b>Common Name</b> 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.
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 <b>Create a self-signed certificate</b> 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 <b>Create a certification request and save it locally for later manual enrollment</b> to have the ZyXEL Device generate and store a request for a certificate. Use the <b>My Certificate Details</b> screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the <b>My Certificate Details</b> screen (see <a href="#">Section 19.7 on page 256</a> ) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select <b>Create a certification request and enroll for a certificate immediately online</b> 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 <b>Trusted CAs</b> 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 <b>Reference Number</b> and <b>Key</b> if the certification authority requires them.

**Table 93** My Certificate Create (continued)

LABEL	DESCRIPTION
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. <b>Simple Certificate Enrollment Protocol (SCEP)</b> is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. <b>Certificate Management Protocol (CMP)</b> 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 <b>CA Certificate</b> drop-down list box. You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen. Click <b>Trusted CAs</b> to go to the <b>Trusted CAs</b> screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication	When you select <b>Create a certification request and enroll for a certificate immediately online</b> , 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 <b>Reference Number</b> and the <b>Key</b> fields if your certification authority uses CMP enrollment protocol. Just fill in the <b>Key</b> field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.
Apply	Click <b>Apply</b> to begin certificate or certification request generation.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyXEL Device is generating the self-signed certificate or certification request.

After the ZyXEL Device successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyXEL Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate 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.

## 19.7 My Certificate Details

Click **Security > Certificates > My Certificates** to open the **My Certificates** screen (see [Figure 135 on page 251](#)). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyXEL Device uses to sign the trusted remote host certificates that you import to the ZyXEL Device.



The following table describes the labels in this screen.

**Table 94** My Certificate Details

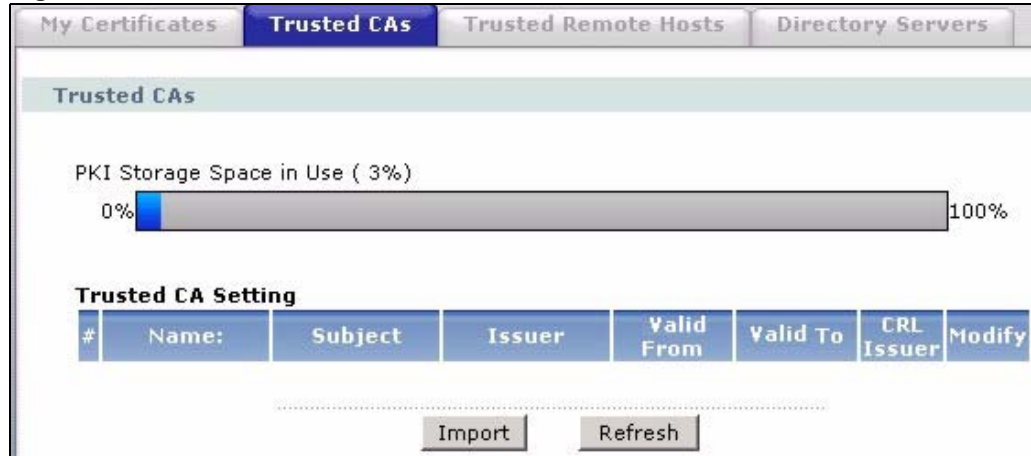
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyXEL Device use this certificate to sign the trusted remote host certificates that you import to the ZyXEL Device. This check box is only available with self-signed certificates.  If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certification Path	Click the <b>Refresh</b> button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).  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 certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyXEL Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click <b>Refresh</b> 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 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 <b>Subject Name</b> 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.

**Table 94** My Certificate Details (continued)

LABEL	DESCRIPTION
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.
Certificate in PEM (Base-64) Encoded Format	<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 button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

## 19.8 Trusted CAs

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

**Figure 139** Trusted CAs

The following table describes the labels in this screen.

**Table 95** 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 <b>Subject</b> 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 <b>Issues certificate revocation lists (CRL)</b> 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 the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.



**Table 95** Trusted CAs (continued)

LABEL	DESCRIPTION
Import	Click <b>Import</b> to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

## 19.9 Trusted CA Import

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device.

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

**Figure 140** Trusted CA Import

The following table describes the labels in this screen.

**Table 96** Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the ZyXEL Device.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.

## 19.10 Trusted CA Details

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

**Figure 141** Trusted CA Details

**Certificates - Trusted CAs - Details**

**Certificate Name**

**Property**  
 Issues certificate revocation lists (CRL)

**Certificate Path**  
 Refresh

**Certificate Informations**

<b>Type</b>	CA-signed X.509 Certificate
<b>Version</b>	V3
<b>Serial Number</b>	-78778323959442690871700631440406797776
<b>Subject</b>	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
<b>Issuer</b>	CN=Root SGC Authority
<b>Signature Algorithm</b>	rsa-pkcs1-md5
<b>Valid From</b>	1999 Aug 20th, 00:30:01 GMT
<b>Valid To</b>	2014 Jan 28th, 07:00:00 GMT
<b>Key Algorithm</b>	rsaEncryption (2048 bits)
<b>MD5 Fingerprint</b>	6f:7e:74:a3:a1:3a:ca:bb:63:cf:74:04:17:05:fa:33
<b>SHA1 Fingerprint</b>	e5:21:5d:34:60:c2:c2:0b:be:2d:9f:e5:fb:66:5d:aa:2c:0e:22:5c

**Certificate in PEM (Base-64) Encoded Format**

```
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIQxLvYwMr/VqURO1aWYZkiMDANBgkqhkiG9w0BAQQFADAd
MRswGQYDVQQDExJSb290IFNHNQYBBdXR0b3JpdHkwHhcNOTkwODIwMDAzMDAxWbcN
MTQwMTI4MDcwMDAwWjBXMQswCQYDVQQGEwJCRTEZMBcGA1UEChMQR2xyYmFsU2ln
biBud11zYTEQMA4GA1UECXMHUUm9vdCBDQTEbMBkGA1UEAxMSR2xyYmFsU2lnbiBS
b290IENBMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAg2g7mmY3Oo+NP
in778YuDJWvqSB/xKrC51REEvfBj0eJnZs8c3c8bSCvujYmOmQ8pgGWr6cctEsur
HEXwB6E9CjDNFY1P+N3UjFAVHO9Q7sQu9/zpUvKRfeBt1TUwj15Dc/JB6dVq47KJ
O1Y5OG8GPIhpWypNxadUuGyJzJv5PMr1/Yn1EjySeJbW3HRukORhOY3HRrJ1Dobo
GYrVbWzVeBaVounICjrr8iQTT3NUKxOFOhu8HjS1iwWMuXeLsdsfIJGrCVNukM57
-----
```

The following table describes the labels in this screen.

**Table 97** Trusted CA Details

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).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certification Path	Click the <b>Refresh</b> button to have this read-only text box display 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.
Refresh	Click <b>Refresh</b> 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 <b>Subject Name</b> 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.

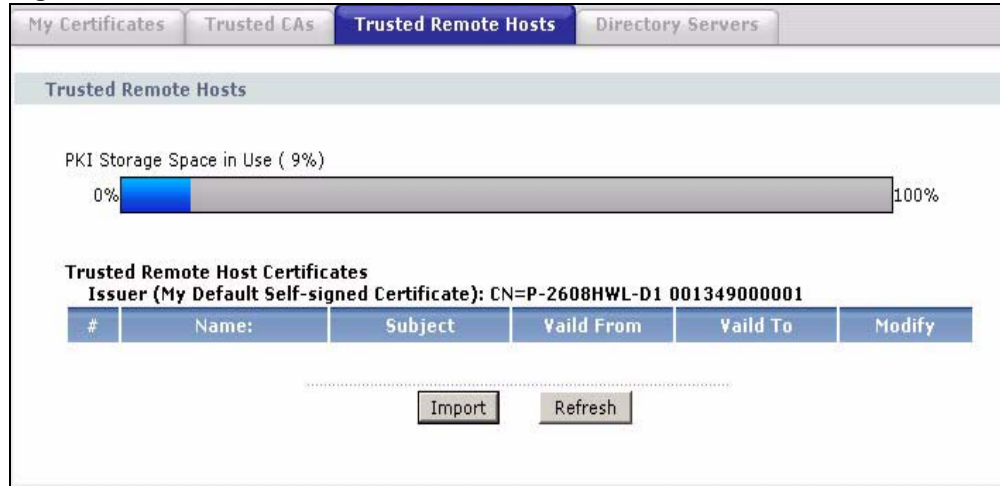
**Table 97** Trusted CA Details (continued)

LABEL	DESCRIPTION
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.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
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 with the certification authority (over the phone for example) that this is actually their 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 with the certification authority (over the phone for example) that this is actually their 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 button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.

## 19.11 Trusted Remote Hosts

Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the 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 142** Trusted Remote Hosts

The following table describes the labels in this screen.

**Table 98** 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 the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Import	Click <b>Import</b> to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

## 19.12 Verifying a Trusted Remote Host's Certificate

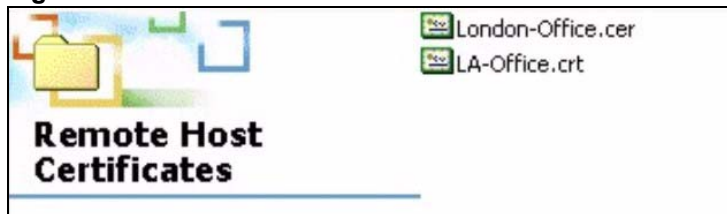
Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

### 19.12.1 Trusted Remote Host Certificate Fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's actual certificate.

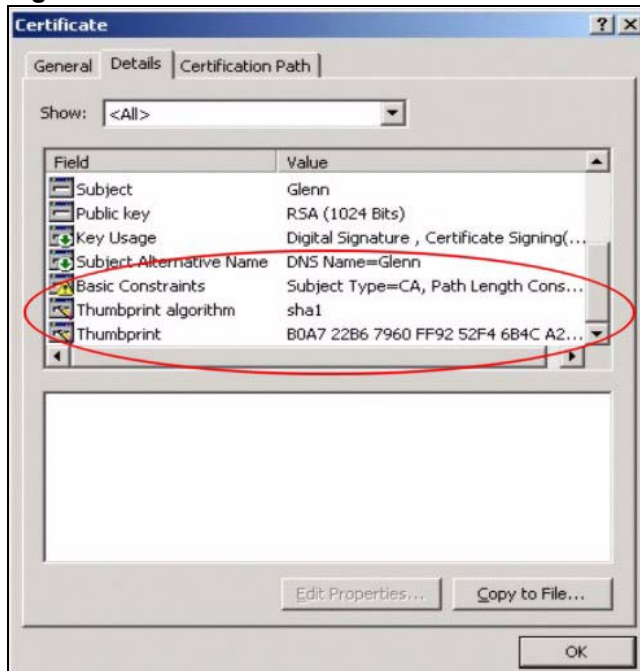
- 1 Browse to where you have the remote host's certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 143 Remote Host Certificates



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 144 Certificate Details



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

## 19.13 Trusted Remote Hosts Import

Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host's certificate to the ZyXEL Device.

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

**Figure 145** Trusted Remote Host Import

The following table describes the labels in this screen.

**Table 99** Trusted Remote Host Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the ZyXEL Device.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted Remote Hosts</b> screen.

## 19.14 Trusted Remote Host Certificate Details

Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

**Figure 146** Trusted Remote Host Details

**Certificates - Trusted Remote Hosts - Details**

**Certificate Name**

**Certificate Path**  
 Refresh

**Certificate Path**

<b>Type</b>	CA-signed X.509 Certificate
<b>Version</b>	V3
<b>Serial Number</b>	144494120486291136762321733029693522805
<b>Subject</b>	CN=ZyZEL
<b>Issuer</b>	CN=P662HW-D1 001349000001
<b>Signature Algorithm</b>	rsa-pkcs1-sha1
<b>Valid From</b>	2005 Sep 2nd, 02:46:18 GMT (Not Yet Valid!)
<b>Valid To</b>	2010 Sep 2nd, 02:54:46 GMT
<b>Key Algorithm</b>	rsaEncryption (2048 bits)
<b>Key Usage</b>	DigitalSignature
<b>Basic Constraint</b>	Path Length Constraint=10
<b>CRL Distribution Points</b>	[1]CRL Distribution Point
<b>MD5 Fingerprint</b>	Full Name: URI=http://zyxel-g97zfcjk2/CertEnroll/ZyZEL.cer, URI=eb:be:19:67:f5:81:ff:be:85:63:66:ff:6d:5b:8a:b7
<b>SHA1 Fingerprint</b>	c5:c0:e9:bd:fe:f0:8f:7d:35:29:49:73:2b:0e:a8:c9:fd:82:90:ca

**Certificate in PEM (Base-64) Encoded Format**

```
-----BEGIN CERTIFICATE-----
MIICvTCCAmegAwIBAgIQbLSOKvmRSaBO2DwzWwyDdTANBgkqhkiG9w0BAQUFADAi
MSAwHgYDVQQDExdQNjYySFctRDEgIDAwMTMOOTAwMDAwMTAeFw0wNTA5MDIwMjQ2
MThaFw0xMDA5MDIwMjU0NDZaMBAxZjAMBgNVBAMTBVp5WkVMMlIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxK04T3OpQHIVMits15IrupkZlFSgg9KR2/tW
FogGTWJ6JVMhuqSybaxTORfd07LqBnLiFP12UZxlrNVvfnPzGwf/Yvj1FPfuo3Nq
Y/6zkySeZSt9HR1zWJ6uC6hwJurPsxZizGvD4E1Ju609VKyhdnX7aCODaN32p8WD
Tc+p+YFhqDVCMOkRmKjQBPgRsMbzxrd0AYRL3ZHe/lmvOdIVZNATVMmHC2Vx9I/
I3O96TIVcUdNI5d93idwxTFhDGB+ogMFGx9nu2XCQL4yuOGntfFmYR3/3icH75r+
tHD3yFacTF1fAojo8WXvc7iWxDm+UGbUg9/U+jKL6Y1PSjxihQIDAQABo4HCMIG/
-----
```



The following table describes the labels in this screen.

**Table 100** Trusted Remote Host Details

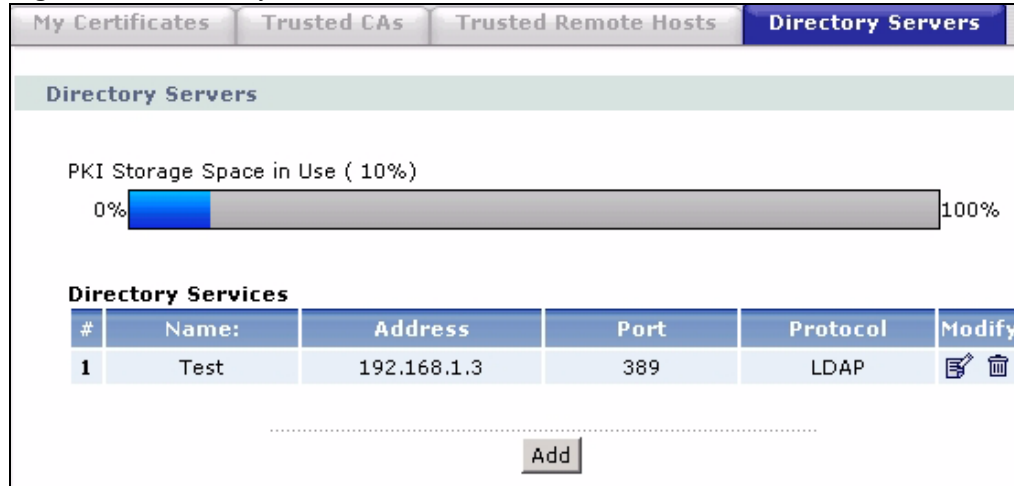
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click the <b>Refresh</b> button to have this read-only text 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 <b>Refresh</b> 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.
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.

**Table 100** Trusted Remote Host Details (continued)

LABEL	DESCRIPTION
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 <a href="#">Section 19.12 on page 266</a> 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 <a href="#">Section 19.12 on page 266</a> 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 button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device. You can only change the name of the certificate.
Cancel	Click <b>Cancel</b> to quit configuring this screen and return to the <b>Trusted Remote Hosts</b> screen.

## 19.15 Directory Servers

Click **Security > Certificates > Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyXEL Device. If you decide to have the ZyXEL Device check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyXEL Device first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyXEL Device checks the servers listed here.

**Figure 147** Directory Servers

The following table describes the labels in this screen.

**Table 101** 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 the details icon to open a screen where you can change the information about the directory server. Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action.
Add	Click <b>Add</b> to open a screen where you can configure information about a directory server so that the ZyXEL Device can access it.

## 19.16 Directory Server Add or Edit

Click **Security > Certificates > Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the **Directory Server Add** screen. Use this screen to configure information about a directory server that the ZyXEL Device can access.

**Figure 148** Directory Server Add

The following table describes the labels in this screen.

**Table 102** Directory Server Add

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server. <b>LDAP</b> (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates. <sup>1</sup>
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 <b>Access Protocol</b> 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).
Back	Click <b>Back</b> to return to the <b>Directory Servers</b> screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to quit configuring this screen.

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

# CHAPTER 20

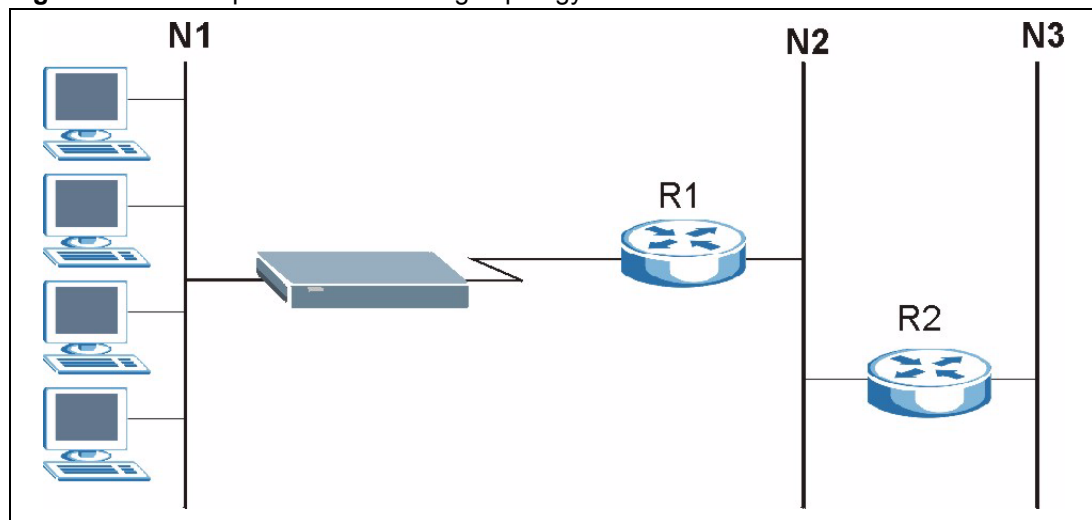
## Static Route

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

### 20.1 Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

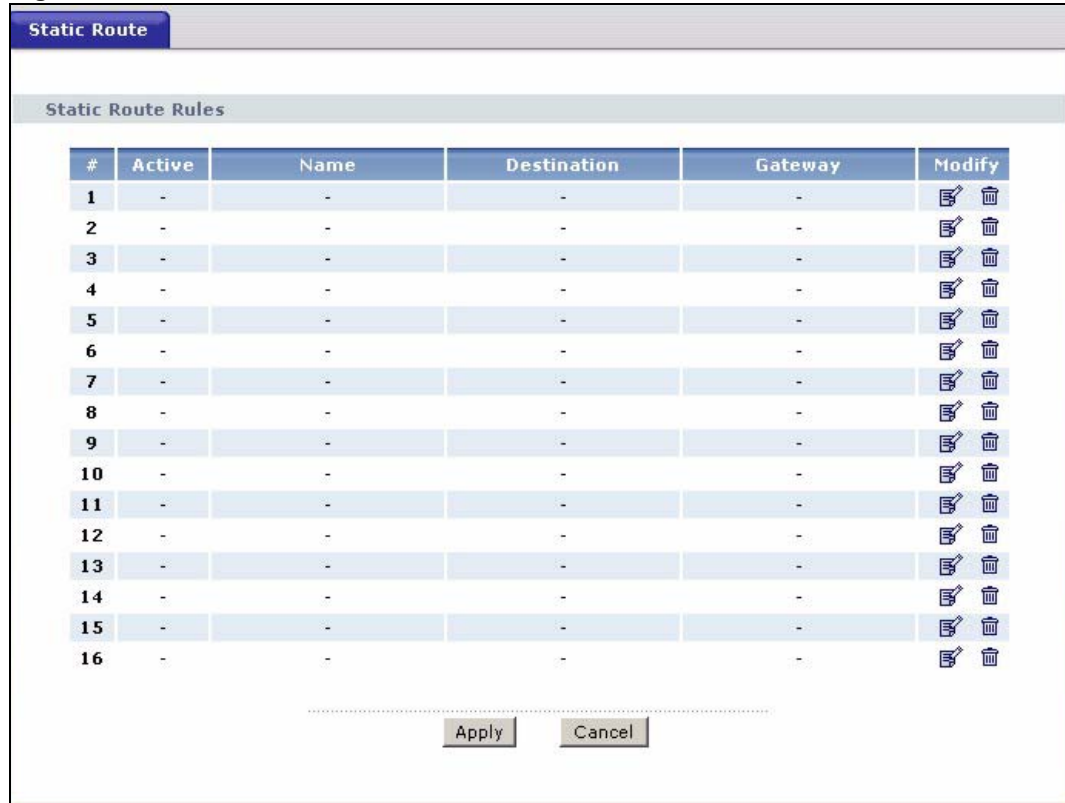
**Figure 149** Example of Static Routing Topology



### 20.2 Configuring Static Route

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

**Figure 150** Static Route



The following table describes the labels in this screen.

**Table 103** Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field shows whether this static route is active ( <b>Yes</b> ) or not ( <b>No</b> ).
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the delete icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.

### 20.2.1 Static Route Edit

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

**Figure 151** Static Route Edit

**Static Route Setup**

Active

Route Name

Destination IP Address

IP Subnet Mask

Gateway IP Address

The following table describes the labels in this screen.

**Table 104** Static Route Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Back	Click <b>Back</b> to return to the previous screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.





# CHAPTER 21

## Bandwidth Management

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

### 21.1 Bandwidth Management Overview

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

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

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

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

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

### 21.2 Application-based Bandwidth Management

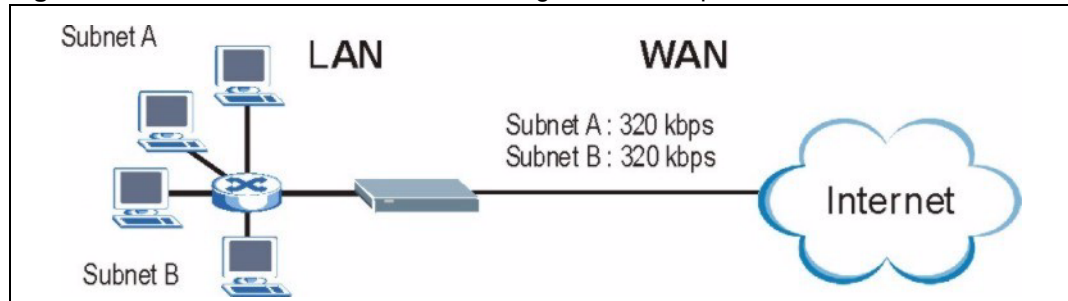
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

### 21.3 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

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

**Figure 152** Subnet-based Bandwidth Management Example



## 21.4 Application and Subnet-based Bandwidth Management

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

**Table 105** Application and Subnet-based Bandwidth Management Example

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

## 21.5 Scheduler

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

### 21.5.1 Priority-based Scheduler

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

## 21.5.2 Fairness-based Scheduler

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

## 21.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see [Figure 153 on page 282](#)) allows the ZyXEL Device to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

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

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

### 21.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

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

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

## 21.6.2 Maximize Bandwidth Usage Example

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

**Table 106** Maximize Bandwidth Usage Example

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

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

### 21.6.2.1 Priority-based Allotment of Unused & Unbudgeted Bandwidth

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

**Table 107** Priority-based Allotment of Unused & Unbudgeted Bandwidth Example

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

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

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

- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

### 21.6.2.2 Fairness-based Allotment of Unused & Unbudgeted Bandwidth

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

**Table 108** Fairness-based Allotment of Unused & Unbudgeted Bandwidth Example

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

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

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

### 21.6.3 Bandwidth Management Priorities

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

**Table 109** Bandwidth Management Priorities

PRIORITY	DESCRIPTION
High	Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).
Mid	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Low	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.

## 21.7 Over Allotment of Bandwidth

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

**Table 110** 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.

## 21.8 Configuring Summary

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

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

**Figure 153** Bandwidth Management: Summary

Summary

BW Manager manages the bandwidth of traffic flowing out of router on the specific interface. BW Manager can be switched on/off independently for each interface.

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

Apply Cancel

The following table describes the labels in this screen.

**Table 111** Media Bandwidth Management: Summary

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

## 21.9 Bandwidth Management Rule Setup

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

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

**Figure 154** Bandwidth Management: Rule Setup

Summary **Rule Setup** Monitor

Rule Setup

Direction  Service  Priority  Bandwidth  (kbps)

To LAN Interface

#	Active	Rule Name	Destination Port	Priority	Bandwidth(kbps)	Modify
1	<input checked="" type="checkbox"/>	WWW	0	High	10	
2	<input checked="" type="checkbox"/>	Telnet	0	Mid	10	

The following table describes the labels in this screen.

**Table 112** Bandwidth Management: Rule Setup

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



**Table 112** Bandwidth Management: Rule Setup (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 rule.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 21.9.1 Rule Configuration

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

**Figure 155** Bandwidth Management Rule Configuration

See [Appendix D on page 387](#) for a list of commonly-used services. The following table describes the labels in this screen.

**Table 113** Bandwidth Management Rule Configuration

LABEL	DESCRIPTION
Rule Configuration	
Active	Select this check box to have the ZyXEL Device apply this bandwidth management rule. Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule. Enabling a bandwidth management rule also allows you to control the maximum amounts of bandwidth that can be used by traffic that matches the rule.

**Table 113** Bandwidth Management Rule Configuration (continued)

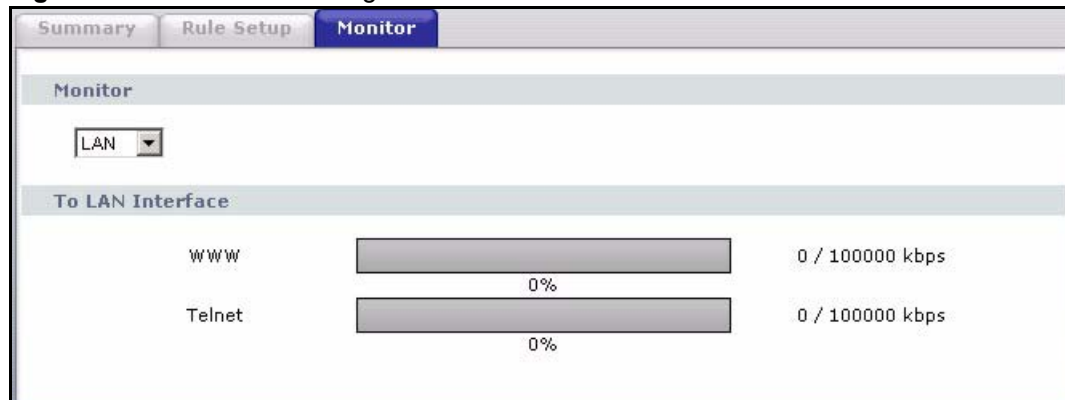
LABEL	DESCRIPTION
Rule Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
BW Budget	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule.
Priority	Select a priority from the drop down list box. Choose <b>High</b> , <b>Mid</b> or <b>Low</b> .
Use All Managed Bandwidth	Select this option to allow a rule to borrow unused bandwidth on the interface. Bandwidth borrowing is governed by the priority of the rules. That is, a rule with the highest priority is the first to borrow bandwidth. Do not select this if you want to leave bandwidth available for other traffic types or if you want to restrict the amount of bandwidth that can be used for the traffic that matches this rule.
Filter Configuration	
Service	<p>This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).</p> <p>SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select <b>SIP</b> from the drop-down list box to configure this bandwidth filter for traffic that uses SIP.</p> <p>File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select <b>FTP</b> from the drop-down list box to configure this bandwidth filter for FTP traffic.</p> <p>H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Select <b>H.323</b> from the drop-down list box to configure this bandwidth filter for traffic that uses H.323.</p> <p>Select <b>User defined</b> from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select <b>User defined</b>, you need to configure at least one of the following fields (other than the <b>Subnet Mask</b> fields which you only enter if you also enter a corresponding destination or source IP address).</p>
Destination Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a <b>Destination Address</b> . Refer to the appendix for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See <a href="#">Appendix A on page 387</a> for some common services and port numbers. A blank destination IP address means any destination IP address.
Source Address	Enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Source Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a <b>Source Address</b> . Refer to the appendix for more information on IP subnetting. A blank source port means any source port number.
Source Port	Enter the port number of the source. See <a href="#">Appendix A on page 387</a> for some common services and port numbers.

**Table 113** Bandwidth Management Rule Configuration (continued)

LABEL	DESCRIPTION
Protocol	Select the protocol ( <b>TCP</b> or <b>UDP</b> ) or select <b>User defined</b> and enter the protocol (service type) number. 0 means any protocol number.
Back	Click <b>Back</b> to go to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 21.10 Bandwidth Monitor

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

**Figure 156** Bandwidth Management: Monitor



# CHAPTER 22

## Dynamic DNS Setup

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

### 22.1 Dynamic DNS Overview

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

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

#### 22.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes \*.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, [www.yourhost.dyndns.org](http://www.yourhost.dyndns.org) and still reach your hostname.

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

See [Section 22.2 on page 289](#) for configuration instruction.

### 22.2 Configuring Dynamic DNS

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

See [Section 22.1 on page 289](#) for more information.

**Figure 157** Dynamic DNS

The following table describes the fields in this screen.

**Table 114** Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when <b>CustomDNS</b> is selected in the <b>DDNS Type</b> field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.

**Table 114** Dynamic DNS (continued)

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP Address	Select this option only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.  <b>Note:</b> The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.





# CHAPTER 23

## Remote Management Configuration

This chapter provides information on configuring remote management.

### 23.1 Remote Management Overview

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

**Note:** When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

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

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

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

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

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

- 1 Console
- 2 Telnet
- 3 HTTPS and HTTP

#### 23.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

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

## 23.1.2 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.

## 23.1.3 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.

## 23.2 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see [Chapter 19 on page 249](#) for more information).

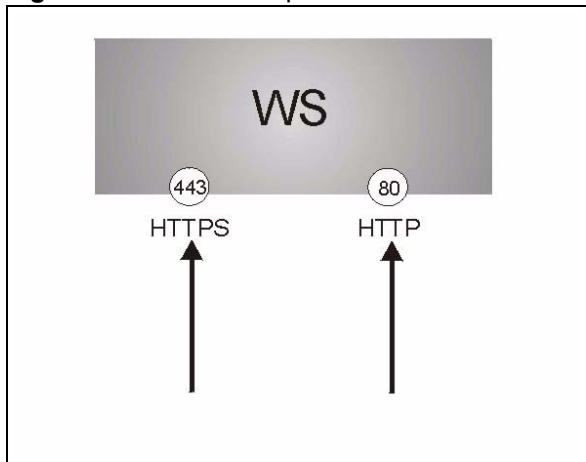
HTTPS on the ZyXEL Device is used so that you may securely access the ZyXEL Device using the web configurator. The SSL protocol specifies that the SSL server (the ZyXEL Device) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT, WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyXEL Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyXEL Device.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyXEL Device's WS (web server).

- 2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyXEL Device's WS (web server).

**Figure 158** HTTPS Implementation



**Note:** If you disable **HTTP Server Access (Disable)** in the **REMOTE MGMT WWW** screen, then the ZyXEL Device blocks all HTTP connection attempts.

## 23.3 WWW

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

**Figure 159** Remote Management: WWW

The screenshot shows the 'WWW' configuration page in the ZyXEL Remote Management interface. The page has tabs for 'WWW', 'Telnet', 'FTP', 'SNMP', 'DNS', and 'ICMP'. The 'WWW' section includes fields for 'Port' (80), 'Access Status' (LAN & WAN), and 'Secured Client IP' (All). The 'HTTPS' section includes 'Server Host Key' (See My Certificates), 'Authenticate Client Certificates' (unchecked), 'Port' (443), 'Access Status' (All), and 'Secured Client IP' (All). A note at the bottom provides instructions for UPnP and Firewall rules. 'Apply' and 'Cancel' buttons are at the bottom.

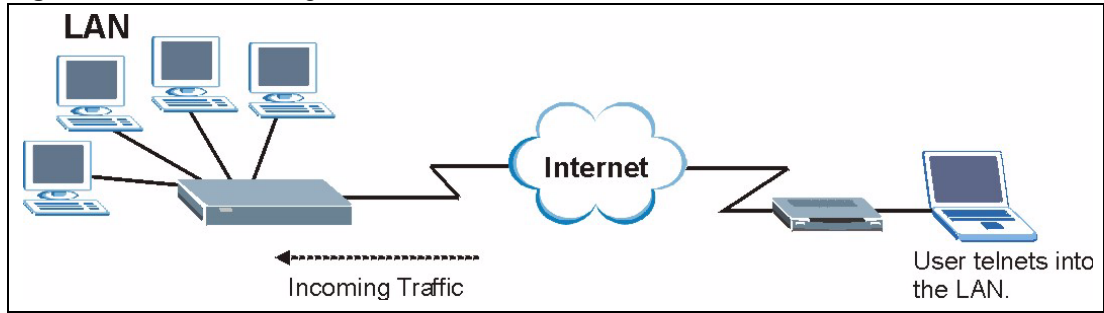
The following table describes the labels in this screen.

**Table 115** Remote Management: WWW

LABEL	DESCRIPTION
WWW	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
HTTPS	
Server Host Key	Select the certificate that the ZyXEL Device will use to identify itself. The ZyXEL Device is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device).
Authenticate Client Certificates	Select <b>Authenticate Client Certificates</b> (optional) to require the SSL client to authenticate itself to the ZyXEL Device by sending the ZyXEL Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyXEL Device (see <a href="#">Appendix E on page 389</a> on importing certificates for details).
Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyXEL Device, for example 8443, then you must notify people who need to access the ZyXEL Device web configurator to use “https://ZyXEL Device IP Address: <b>8443</b> ” as the URL.
Access Status	Select a ZyXEL Device interface from <b>Access Status</b> on which incoming HTTPS access is allowed. You can allow only secure web configurator access by setting the <b>WWW Access Status</b> field to <b>Disable</b> and setting the <b>HTTPS Access Status</b> field to an interface(s).
Secure Client IP	A secure client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click <b>Apply</b> to save your settings back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.4 Telnet

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

**Figure 160** Telnet Configuration on a TCP/IP Network

## 23.5 Configuring Telnet

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

**Figure 161** Remote Management: Telnet

The following table describes the labels in this screen.

**Table 116** Remote Management: Telnet

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

## 23.6 Configuring FTP

You can upload and download the ZyXEL Device's firmware and configuration files using FTP, please see [Chapter 27 on page 331](#) for details. To use this feature, your computer must have an FTP client.

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

**Figure 162** Remote Management: FTP

The following table describes the labels in this screen.

**Table 117** Remote Management: FTP

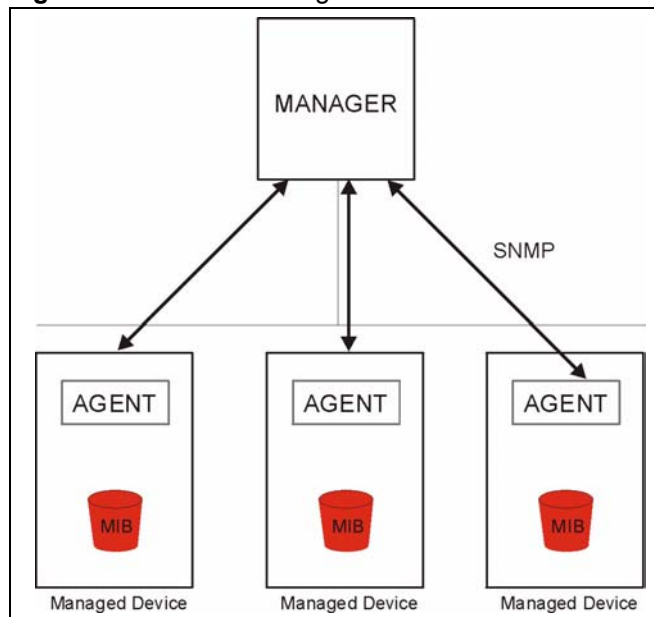
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client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

## 23.7 SNMP

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

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

**Figure 163** 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.

### 23.7.1 Supported MIBs

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

### 23.7.2 SNMP Traps

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

**Table 118** SNMP Traps

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

### 23.7.3 Configuring SNMP

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



**Figure 164** Remote Management: SNMP

The following table describes the labels in this screen.

**Table 119** Remote Management: SNMP

LABEL	DESCRIPTION
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
SNMP Configuration	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.8 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to [Chapter 8 on page 105](#) for background information.

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

**Figure 165** Remote Management: DNS

The screenshot shows the 'DNS' configuration page. At the top, there are navigation tabs: WWW, Telnet, FTP, SNMP, DNS (highlighted), and ICMP. Below the tabs, the 'DNS' section contains the following fields and options:

- Port:** A text box containing the value '53'.
- Access Status:** A dropdown menu currently set to 'LAN & WAN'.
- Secured Client IP:** Radio buttons for 'All' (selected) and 'Selected', followed by a text box containing '0.0.0.0'.
- Note:** A yellow note icon followed by the text: 'Note : You may also need to create a [Firewallrule](#)'.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom.

The following table describes the labels in this screen.

**Table 120** Remote Management: DNS

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

## 23.9 Configuring ICMP

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

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

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

**Figure 166** Remote Management: ICMP

The following table describes the labels in this screen.

**Table 121** Remote Management: ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Otherwise select <b>LAN &amp; WAN</b> to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. By default this option is not selected and the ZyXEL Device will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports.  Note that the probing packets must first traverse the ZyXEL Device's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyXEL Device reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.10 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 122 on page 304](#) for detailed descriptions of the commands.

**Figure 167** 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 122** TR-069 Commands

Root	Command or Subdirectory	Command	Description
wan	tr069		All TR-069 related commands must be preceded by <code>wan tr069</code> .
		load	Start configuring TR-069 on your ZyXEL Device.
		active [0:no/ 1:yes]	Enable/disable TR-069 operation.
		acsUrl <URL>	Set the IP address or domain name of CNM Access.
		username [maxlength:15]	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.
		password [maxlength:15]	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.

**Table 122** TR-069 Commands

Root	Command or Subdirectory	Command	Description
		periodicEnable [0:Disable/ 1:Enable]	Whether or not the device must periodically send information to CNM Access. It is recommended to set this value to 1 in order for the ZyXEL Device to send information to CNM Access.
		informInterval [sec]	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.
		save	Save the TR-069 settings to your ZyXEL Device.



# CHAPTER 24

## Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

### 24.1 Introducing Universal Plug and Play

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

See [Section 24.2.1 on page 308](#) for configuration instructions.

#### 24.1.1 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.

#### 24.1.2 NAT Traversal

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

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

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

See [Chapter 10 on page 139](#) for more information on NAT.

### 24.1.3 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.

## 24.2 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.

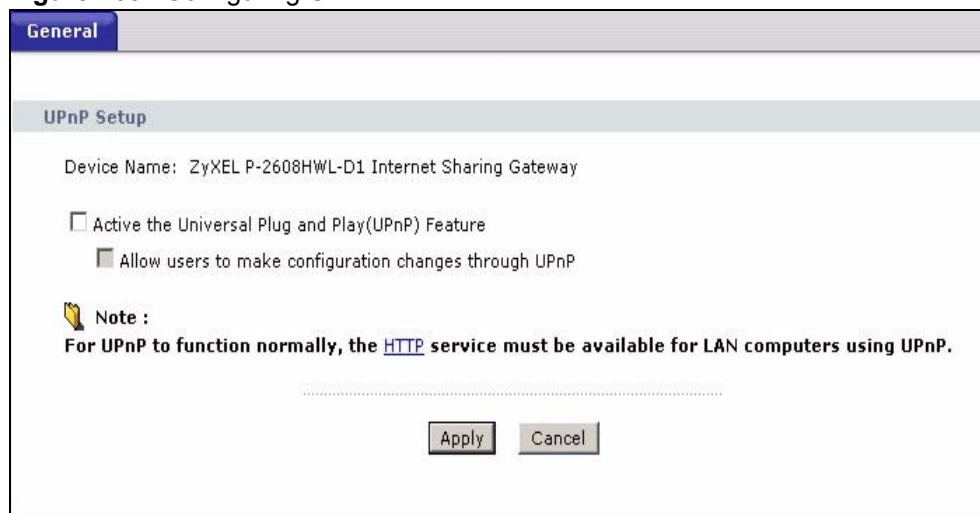
See the following sections for examples of installing and using UPnP.

### 24.2.1 Configuring UPnP

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

See [Section 24.1 on page 307](#) for more information.

**Figure 168** Configuring UPnP



The screenshot shows the 'UPnP Setup' configuration page. At the top, there is a 'General' tab. Below it, the 'UPnP Setup' section is visible. The 'Device Name' is set to 'ZyXEL P-2608HWL-D1 Internet Sharing Gateway'. There are two checkboxes: 'Active the Universal Plug and Play(UPnP) Feature' (unchecked) and 'Allow users to make configuration changes through UPnP' (checked). A note icon is present, followed by the text: 'Note : For UPnP to function normally, the [HTTP](#) service must be available for LAN computers using UPnP.' At the bottom, there are 'Apply' and 'Cancel' buttons.



The following table describes the fields in this screen.

**Table 123** Configuring UPnP

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

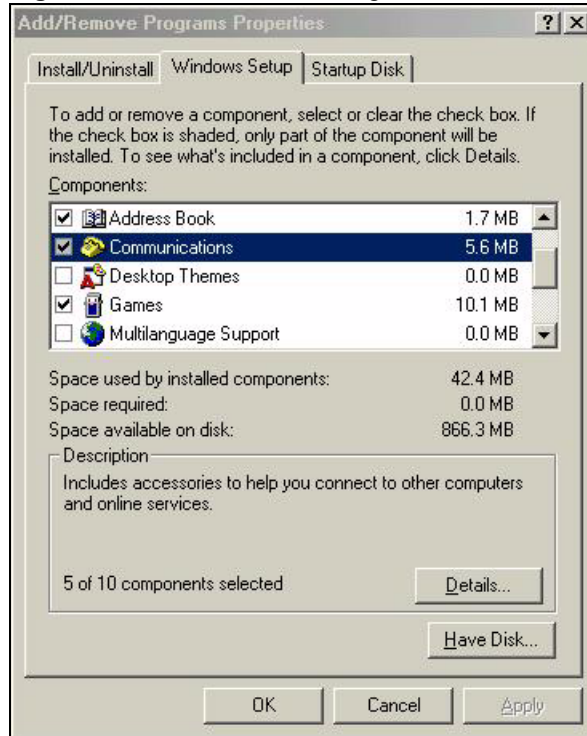
## 24.3 Installing UPnP in Windows Example

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

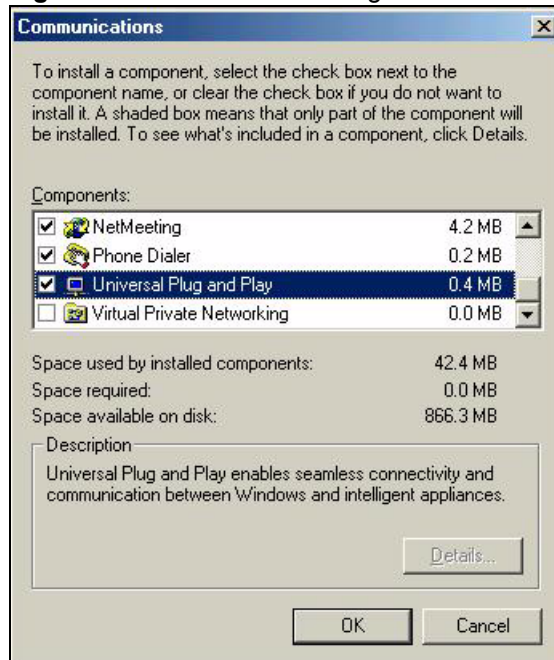
### Installing UPnP in Windows Me

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

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

**Figure 169** 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 170** 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.

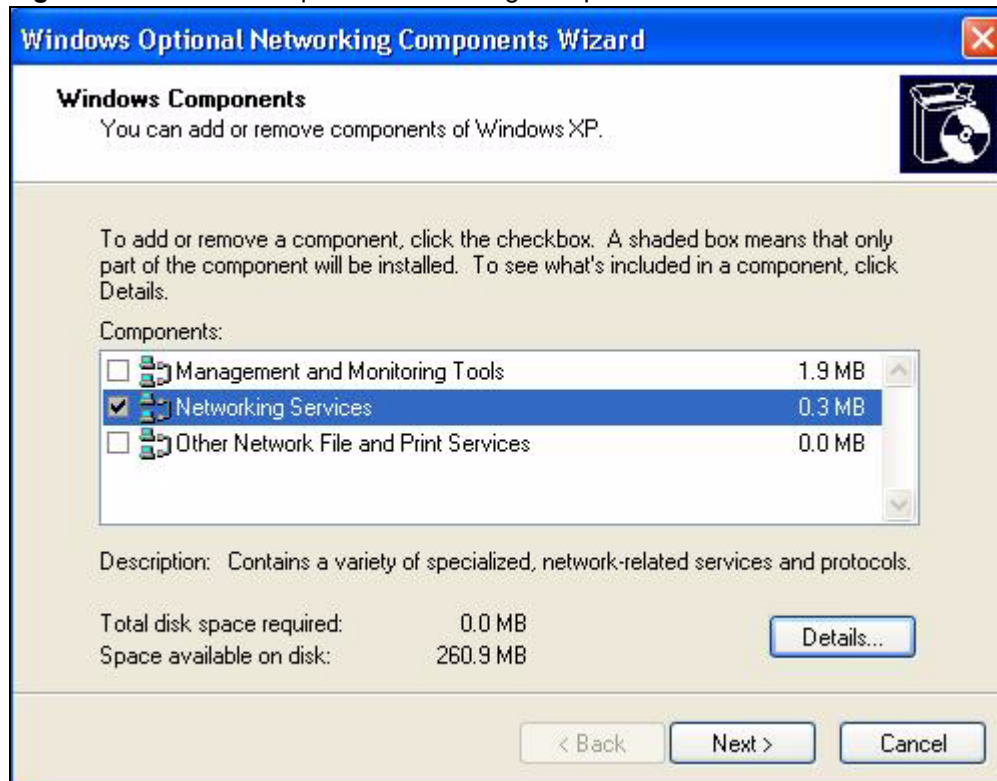
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ....**

**Figure 171** Network Connections

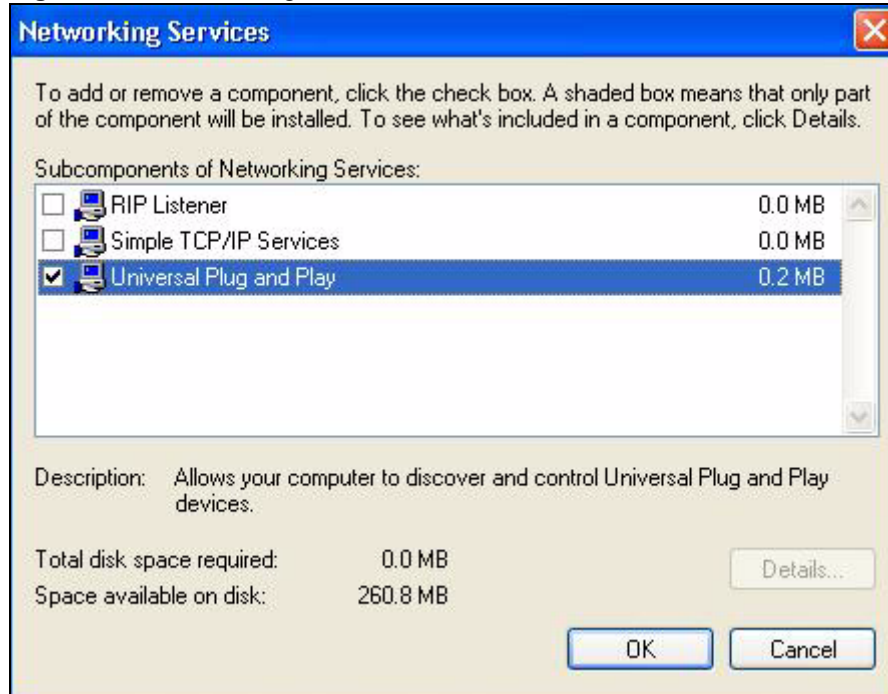


- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 172** Windows Optional Networking Components Wizard



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

**Figure 173** Networking Services

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

## 24.4 Using UPnP in Windows XP Example

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

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

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

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

Figure 174 Network Connections



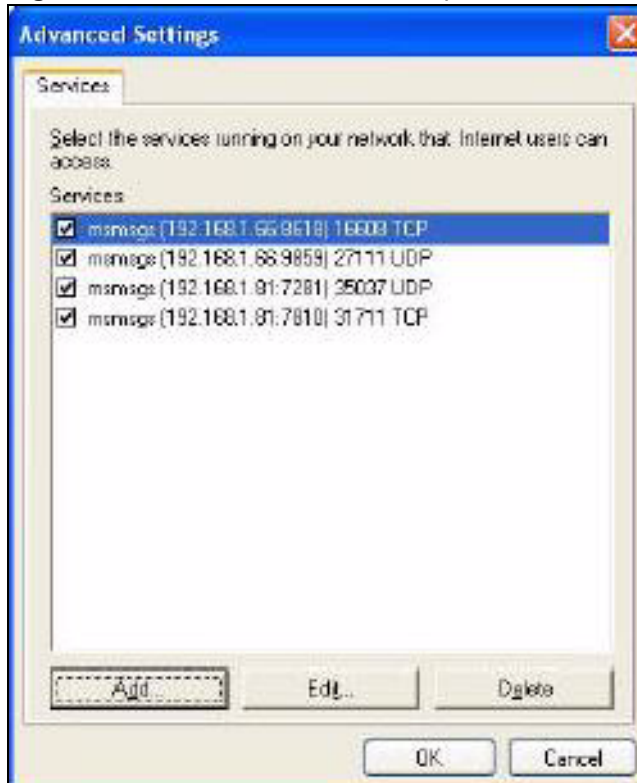
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 175 Internet Connection Properties

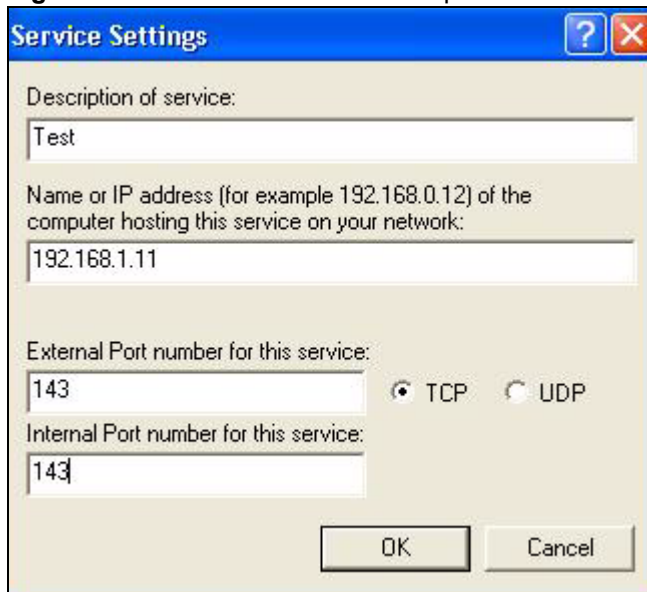


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

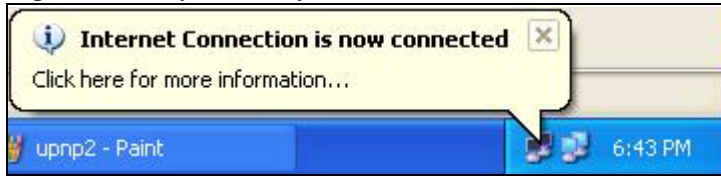
**Figure 176** Internet Connection Properties: Advanced Settings



**Figure 177** 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 178** System Tray Icon

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

**Figure 179** Internet Connection Status

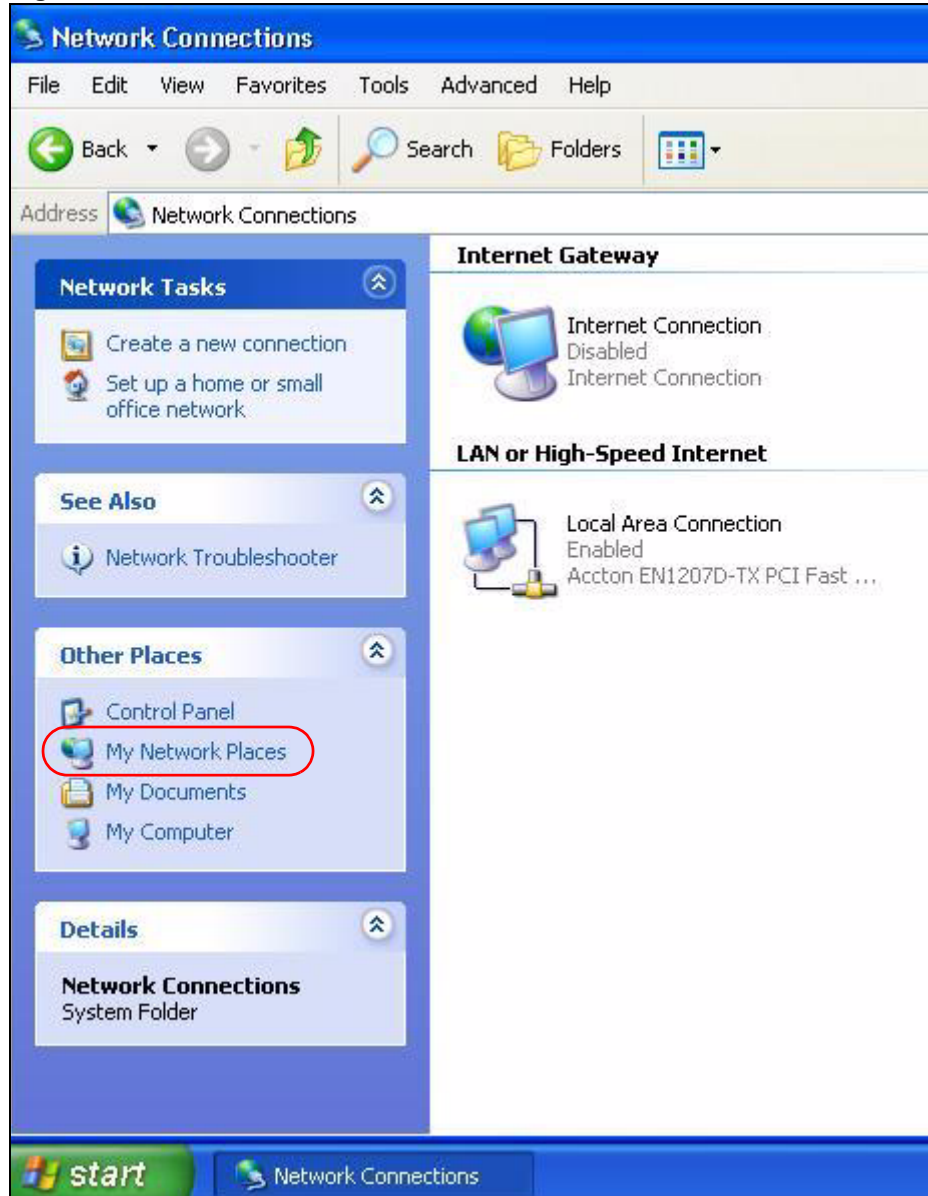
### Web Configurator Easy Access

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.

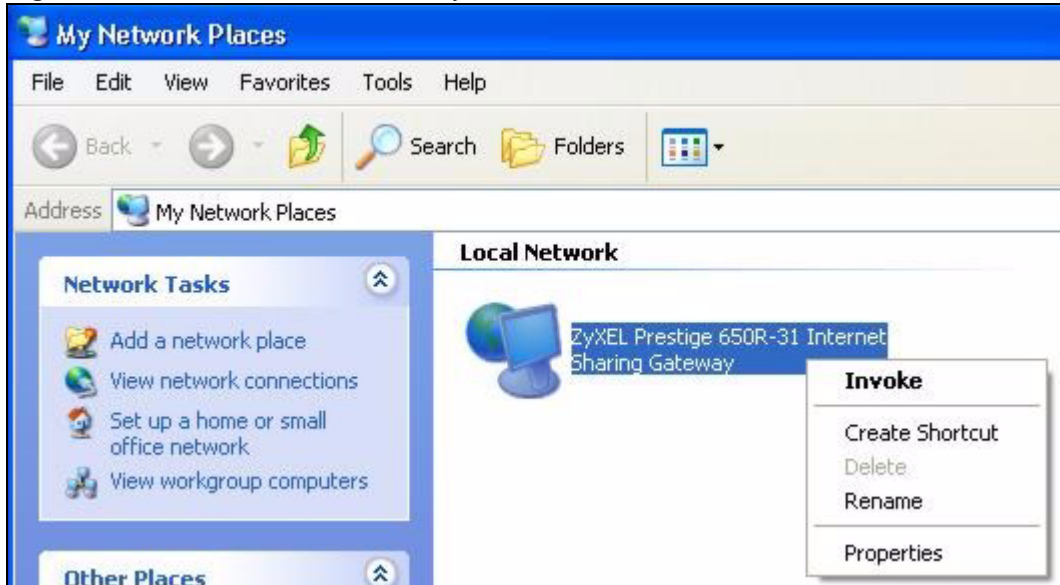
- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.



**Figure 180** 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 181** 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 182** Network Connections: My Network Places: Properties: Example



# CHAPTER 25

## System

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

### 25.1 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**.

#### 25.1.1 General Setup

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

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

**Figure 183** System General Setup

The following table describes the labels in this screen.

**Table 124** System General Setup

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

## 25.2 Time Setting

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

**Figure 184** System Time Setting

The following table describes the fields in this screen.

**Table 125** System Time Setting

LABEL	DESCRIPTION
Current Time	
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 to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.

**Table 125** System Time Setting (continued)

LABEL	DESCRIPTION
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .
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 <b>Time and Date Setup</b> to <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .
Get from Time Server	Select this to have the ZyXEL Device get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. <b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server. <b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, <b>NTP (RFC 1305)</b> , 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.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected <b>Enable Daylight Saving</b> . The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, April</b> and type 2 in the <b>o'clock</b> field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b> . The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

**Table 125** System Time Setting (continued)

LABEL	DESCRIPTION
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Enable Daylight Saving</b>. The <b>o'clock</b> 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 <b>Last, Sunday, October</b> and type 2 in the <b>o'clock</b> 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 <b>Last, Sunday, October</b>. The time you type in the <b>o'clock</b> 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 <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.





# CHAPTER 26

## Logs

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

### 26.1 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.

#### 26.1.1 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.

### 26.2 Viewing the Logs

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 26.3 on page 326](#)).

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

**Figure 185** View Log

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

The following table describes the fields in this screen.

**Table 126** View Log

LABEL	DESCRIPTION
Display	The categories that you select in the <b>Log Settings</b> screen display in the drop-down list box. Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page.
Email Log Now	Click <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page (make sure that you have first filled in the <b>E-mail Log Settings</b> fields in <b>Log Settings</b> ).
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

## 26.3 Configuring Log Settings

Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device is to record. See [Section 26.1 on page 325](#) for more information.

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

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

**Figure 186** Log Settings

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

- E-mail Log Settings:** Contains input fields for 'Mail Server' (with a hint '(Outgoing SMTP Server Name or IP Address)'), 'Mail Subject', 'Send Log to' (with a hint '(E-Mail Address)'), and 'Send Alerts to' (with a hint '(E-Mail Address)'). It also includes a checkbox for 'Enable SMTP Authentication' with sub-fields for 'User Name' and 'Password'. Other options include a dropdown for 'Log Schedule' (set to 'None'), a dropdown for 'Day for Sending Log' (set to 'Monday'), and numeric input fields for 'Time for Sending Log' (0 hour, 0 minute). A checkbox 'Clear log after sending mail' is also present.
- Syslog Logging:** Features a checkbox for 'Active', a text field for 'Syslog IP Address' (set to '0.0.0.0' with a hint '(Server Name or IP Address)'), and a dropdown for 'Log Facility' (set to 'Local 1').
- Active Log and Alert:** Divided into two columns. The 'Log' column has checkboxes for System Maintenance, System Errors, Access Control, UPnP, Forward Web Sites, Blocked Web Sites, Attacks, IPSec, IKE, Any IP, PKI, 802.1x, SIP, RTP, and FSM. The 'Send Immediate Alert' column has checkboxes for System Errors, Access Control, Blocked Web Sites, Attacks, IPSec, IKE, and PKI.

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

The following table describes the fields in this screen.

**Table 127** 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 127** 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	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> <li>• <b>Daily</b></li> <li>• <b>Weekly</b></li> <li>• <b>Hourly</b></li> <li>• <b>When Log is Full</b></li> <li>• <b>None.</b></li> </ul> <p>If you select <b>Weekly</b> or <b>Daily</b>, specify a time of day when the E-mail should be sent. If you select <b>Weekly</b>, then also specify which day of the week the E-mail should be sent. If you select <b>When Log is Full</b>, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are sent.</p>
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click <b>Active</b> to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 26.4 SMTP Error Messages

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

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

**Table 128** SMTP Error Messages

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

### 26.4.1 Example E-mail Log

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

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

**Figure 187 E-mail Log Example**

```

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

```

# CHAPTER 27

## Tools

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

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

### 27.1 Introduction

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

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

### 27.2 Filename Conventions

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

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

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

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

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

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

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

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

**Table 129** Filename Conventions

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

## 27.3 File Maintenance Over WAN

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

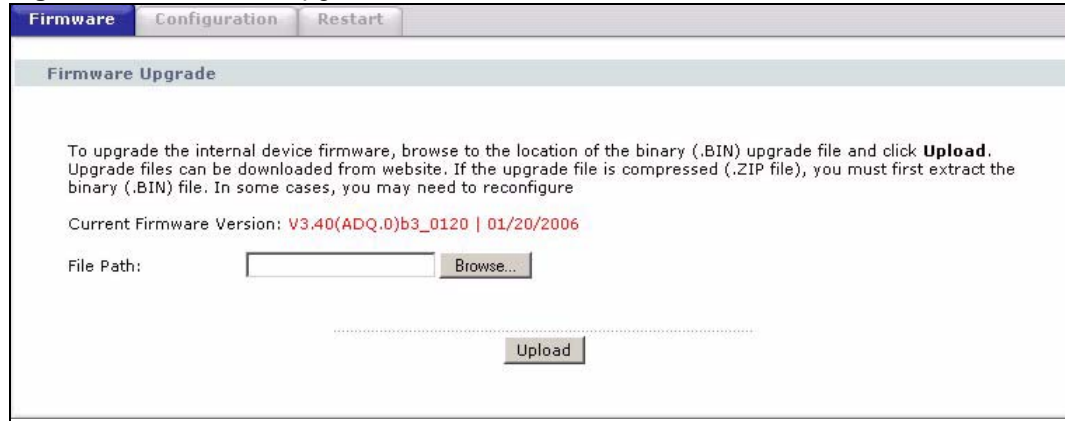
- 1 The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
- 2 You have disabled Telnet service in menu 24.11.
- 3 You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- 4 The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the device will disconnect the Telnet session immediately.

## 27.4 Firmware Upgrade Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See [Section 27.9 on page 341](#) for upgrading firmware using FTP/TFTP commands.



**Figure 188** Firmware Upgrade



The following table describes the labels in this screen.

**Table 130** Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

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

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

**Figure 189** Firmware Upload In Progress



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

**Figure 190** Network Temporarily Disconnected

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

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

**Figure 191** Error Message

## 27.5 Backup and Restore

See [Section 27.7 on page 337](#) and [Section 27.8 on page 340](#) for transferring configuration files using FTP/TFTP commands.

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

**Figure 192** Configuration

The screenshot shows a web interface with three tabs: **Firmware**, **Configuration** (selected), and **Restart**. The **Configuration** section is divided into three sub-sections:

- Backup Configuration:** Contains the instruction "Click **Backup** to save the current configuration to you computer." and a **Backup** button.
- Restore Configuration:** Contains the instruction "To restore a previously saved configuration file on your computer to the Prestige, please type a location for storing the configuration file or click **Browse** to look for one, and then click **Upload**." It includes a "File Path:" input field, a **Browse...** button, and an **Upload** button.
- Reset to Factory Default Settings:** Contains the instruction "Click **Reset** to clear all user-entered configuration and return the Prestige to the factory default settings." It lists default settings: "The following default settings would become effective after click **Reset**  
Password :1234  
Lan IP : 192.168.1.1  
DHCP : Server ." and a **Reset** button.

## 27.5.1 Backup Configuration

Backup Configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

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

## 27.5.2 Restore Configuration

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

**Table 131** Restore Configuration

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

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

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

**Figure 193** Configuration Upload Successful



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

**Figure 194** Network Temporarily Disconnected

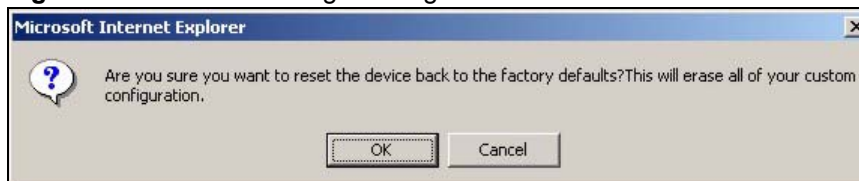


If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See [Appendix B on page 367](#) for details on how to set up your computer's IP address.

### 27.5.3 Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

**Figure 195** Reset Warning Message



**Figure 196** Reset In Process Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to [Section 2.1.2 on page 48](#) for more information on the **RESET** button.

## 27.6 Restart

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

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

**Figure 197** Restart Screen

## 27.7 Using FTP or TFTP to Back Up Configuration

This section covers how to use FTP or TFTP to save your device's configuration file to your computer.

### 27.7.1 Using the FTP Commands to Back Up Configuration

- 1 Launch the FTP client on your computer.
- 2 Enter "open", followed by a space and the IP address of your ZyXEL Device.
- 3 Press [ENTER] when prompted for a username.

- 4 Enter your password as requested (the default is "1234").
- 5 Enter "bin" to set transfer mode to binary.
- 6 Use "get" to transfer files from the ZyXEL Device to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the ZyXEL Device to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.
- 7 Enter "quit" to exit the ftp prompt.

## 27.7.2 FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device's configuration onto your computer.

**Figure 198** FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

## 27.7.3 Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

**Table 132** General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

## 27.7.4 Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

- 1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Enter command “`sys stdio 0`” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command “`sys stdio 5`” to restore the five-minute management idle timeout (default) when the file transfer is complete.
- 3 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
- 4 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is “`rom-0`” (rom-zero, not capital o).

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “`get`” to transfer from the ZyXEL Device to the computer and “`binary`” to set binary transfer mode.

## 27.7.5 TFTP Command Configuration Backup Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where “`i`” specifies binary image transfer mode (use this mode when transferring binary files), “`host`” is the ZyXEL Device IP address, “`get`” transfers the file source on the ZyXEL Device (`rom-0`, name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it `config.rom`.

## 27.7.6 Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

**Table 133** General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.1 is the ZyXEL Device's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyXEL Device and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to [Section 27.3 on page 332](#) to read about configurations that disallow TFTP and FTP over WAN.

## 27.8 Using FTP or TFTP to Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

**Note:** WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR device. When the Restore Configuration process is complete, the device will automatically restart.



## 27.8.1 Restore Using FTP Session Example

**Figure 199** Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to [Section 27.3 on page 332](#) to read about configurations that disallow TFTP and FTP over WAN.

## 27.9 FTP and TFTP Firmware and Configuration File Uploads

This section shows you how to upload firmware and configuration files.

**Note:** WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyxEL Device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

### 27.9.1 FTP File Upload Command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your device.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

## 27.9.2 FTP Session Example of Firmware File Upload

**Figure 200** FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to [Section 27.3 on page 332](#) to read about configurations that disallow TFTP and FTP over WAN.

## 27.9.3 TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

- 1** Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2** Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
- 3** Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
- 4** Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

## 27.9.4 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.



# CHAPTER 28

## Diagnostic

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

### 28.1 General Diagnostic

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

**Figure 201** Diagnostic: General

The screenshot shows a web interface for the 'Diagnostic: General' screen. It features two tabs at the top: 'General' and 'DSL Line'. The 'General' tab is active. Below the tabs, there is a header 'General' and a large text area containing '- Info -'. At the bottom, there is a 'TCP/IP Address' input field and a 'Ping' button.

The following table describes the fields in this screen.

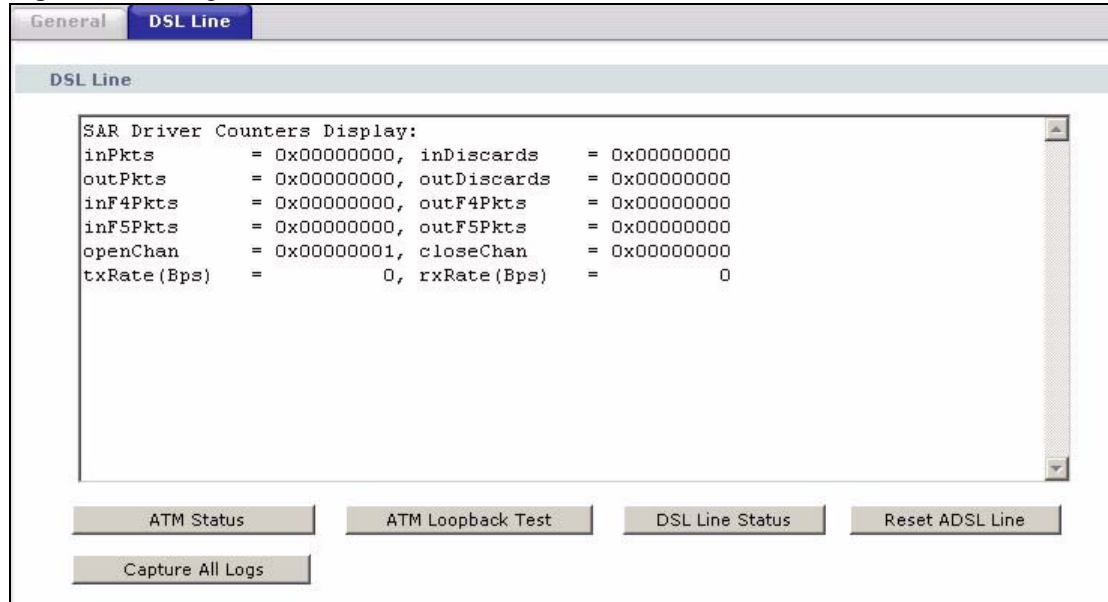
**Table 134** Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.

### 28.2 DSL Line Diagnostic

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

**Figure 202** Diagnostic: DSL Line



The following table describes the fields in this screen.

**Table 135** Diagnostic: DSL Line

LABEL	DESCRIPTION
ATM Status	<p>Click this button to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed.</p> <p>The SAR driver is</p> <p>These counters are set back to zero whenever the device</p> <p><b>inPkts</b> is the number of good ATM cells that have been received.</p> <p><b>inDiscards</b> is the number of received ATM cells that were rejected.</p> <p><b>outPkts</b> is the number of ATM cells that have been sent.</p> <p><b>outDiscards</b> is the number of ATM cells sent that were rejected.</p> <p><b>inF4Pkts</b> is the number of ATM Operations, Administration, and Management (OAM) F4 cells that have been received. See ITU recommendation I.610 for more on OAM for ATM.</p> <p><b>outF4Pkts</b> is the number of ATM OAM F4 cells that have been sent.</p> <p><b>inF5Pkts</b> is the number of ATM OAM F5 cells that have been received.</p> <p><b>outF5Pkts</b> is the number of ATM OAM F5 cells that have been sent.</p> <p><b>openChan</b> is the number of times that the ZyXEL Device has opened a logical DSL channel.</p> <p><b>closeChan</b> is the number of times that the ZyXEL Device has closed a logical DSL channel.</p> <p><b>txRate</b> is the number of bytes transmitted per second.</p> <p><b>rxRate</b> is the number of bytes received per second.</p>
ATM Loopback Test	<p>Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCI before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.</p>

**Table 135** Diagnostic: DSL Line (continued)

LABEL	DESCRIPTION
DSL Line Status	<p>Click this button to view statistics about the DSL connections.</p> <p><b>noise margin downstream</b> is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is.</p> <p><b>output power upstream</b> is the amount of power (in decibels) that the ZyXEL Device is using to transmit to the ISP.</p> <p><b>attenuation downstream</b> is the reduction in amplitude (in decibels) of the DSL signal coming into the ZyXEL Device from the ISP.</p> <p>Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT.</p> <p>The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.</p>
Reset ADSL Line	<p>Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:</p> <pre> "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!" </pre>
Capture All Logs	Click this button to display all logs generated by the DSL line.





# CHAPTER 29

## Troubleshooting

This chapter covers potential problems and the corresponding remedies.

### 29.1 Problems Starting Up the ZyXEL Device

**Table 136** Troubleshooting Starting Up Your Device

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

### 29.2 Problems with the LAN

**Table 137** Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device from the LAN.	If <b>Any IP</b> is disabled, make sure that the IP address and the subnet mask of the ZyXEL Device and your computer(s) are on the same subnet.

## 29.3 Problems with the WAN

**Table 138** Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The <b>DSL</b> light is off.	Check the telephone wire and connections between the ZyXEL Device <b>DSL</b> port and the wall jack.
	Make sure that the telephone company has checked your phone line and set it up for DSL service.
	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to <a href="#">Section 28.2 on page 345</a> .
I cannot get a WAN IP address from the ISP.	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name. The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct <b>Service Type</b> , <b>User Name</b> and <b>Password</b> (be sure to use the correct case). Refer to <a href="#">Section 7.5 on page 94</a> .
I cannot access the Internet.	Make sure the ZyXEL Device is turned on and connected to the network. Verify your WAN settings. Refer to <a href="#">Chapter 7 on page 89</a> . Make sure you entered the correct user name and password. If you use PPPoE pass through, make sure that bridge mode is turned on.
The Internet connection disconnects.	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to <a href="#">Section 7.5 on page 94</a> . Contact your ISP.

## 29.4 Problems Accessing the ZyXEL Device

**Table 139** Troubleshooting Accessing Your Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	<p>The username is "admin". The default password is "1234". The <b>Password</b> and <b>Username</b> fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.</p> <p>If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.</p>
I cannot access the web configurator.	<p>Make sure that there is not a telnet session running.</p> <p>Use the ZyXEL Device's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection.</p> <p>Use the ZyXEL Device's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection.</p> <p>Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to <a href="#">Chapter 23 on page 293</a> for details.</p> <p>Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p>
I cannot remotely manage the ZyXEL Device from the LAN or WAN.	<p>You may also need to clear your Internet browser's cache.</p> <p>In Internet Explorer, click <b>Tools</b> and then <b>Internet Options</b> to open the <b>Internet Options</b> screen.</p> <p>In the <b>General</b> tab, click <b>Delete Files</b>. In the pop-up window, select the <b>Delete all offline content</b> check box and click <b>OK</b>. Click <b>OK</b> in the <b>Internet Options</b> screen to close it.</p> <p>If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).</p> <p>In Windows, use <b>arp -d</b> at the command prompt to delete all entries in your computer's ARP table.</p>
	<p>Refer to <a href="#">Chapter 23 on page 293</a> for scenarios when remote management may not be possible.</p>
	<p>Use the ZyXEL Device's WAN IP address when configuring from the WAN.</p> <p>Use the ZyXEL Device's LAN IP address when configuring from the LAN.</p>

### 29.4.1 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.

### 29.4.1.1 Internet Explorer Pop-up Blockers

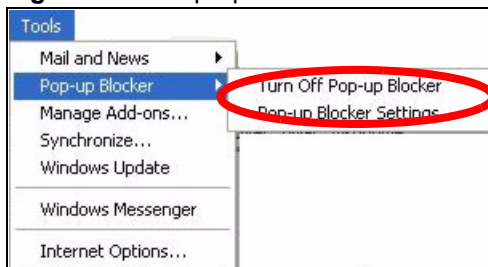
You may have to disable pop-up blocking to log into your device.

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.

#### 29.4.1.1.1 Disable pop-up Blockers

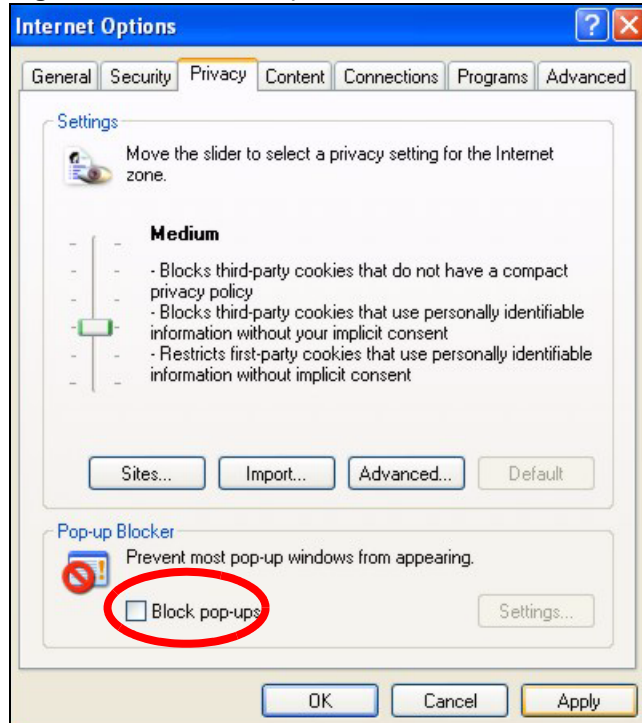
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 203** 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.

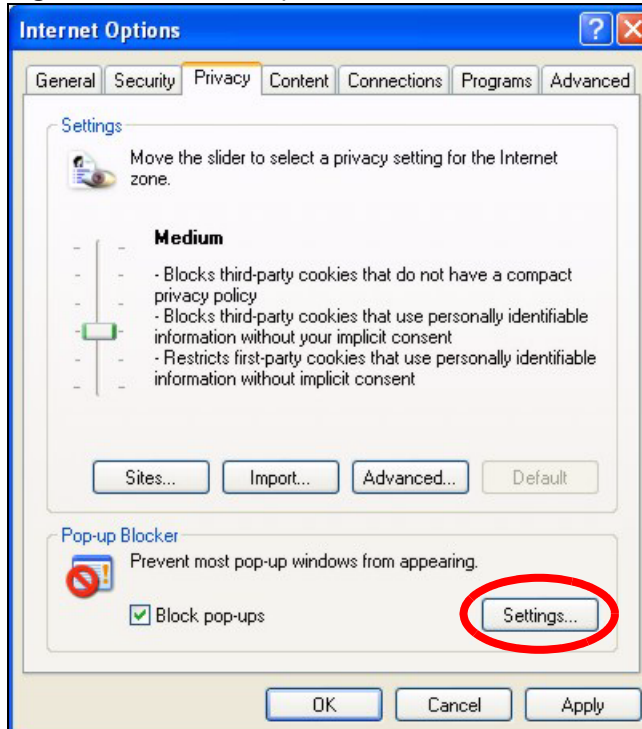
**Figure 204** Internet Options

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

#### 29.4.1.1.2 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 205** 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 206** Pop-up Blocker Settings

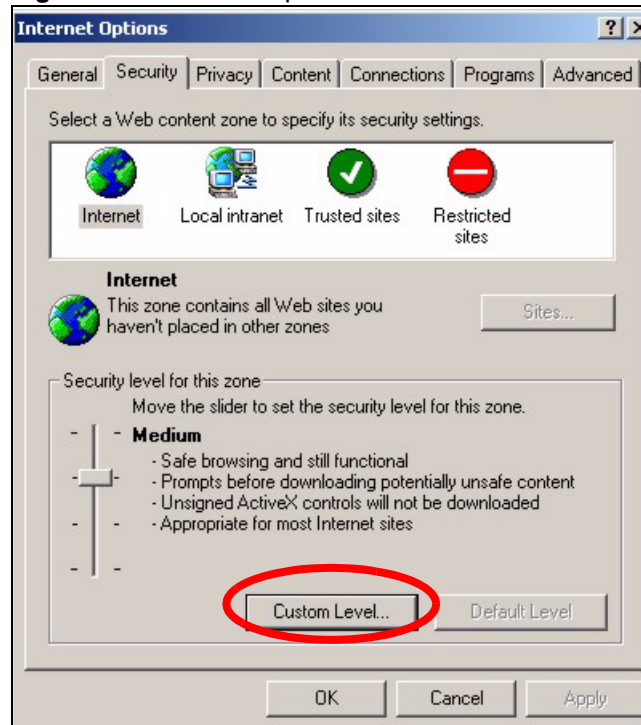
**5** Click **Close** to return to the **Privacy** screen.

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

### 29.4.1.2 JavaScripts

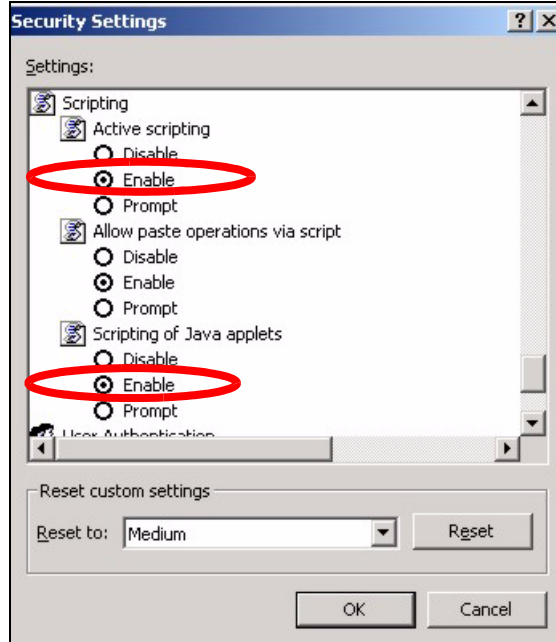
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

**Figure 207** Internet Options

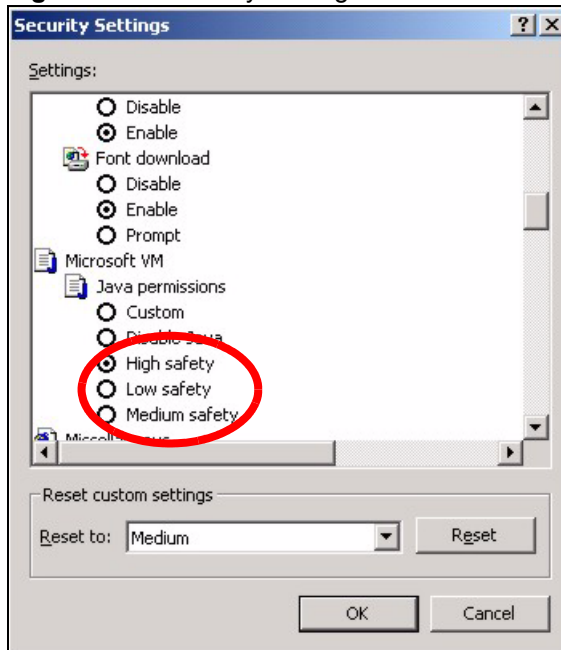
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.



**Figure 208** Security Settings - Java Scripting

### 29.4.1.3 Java Permissions

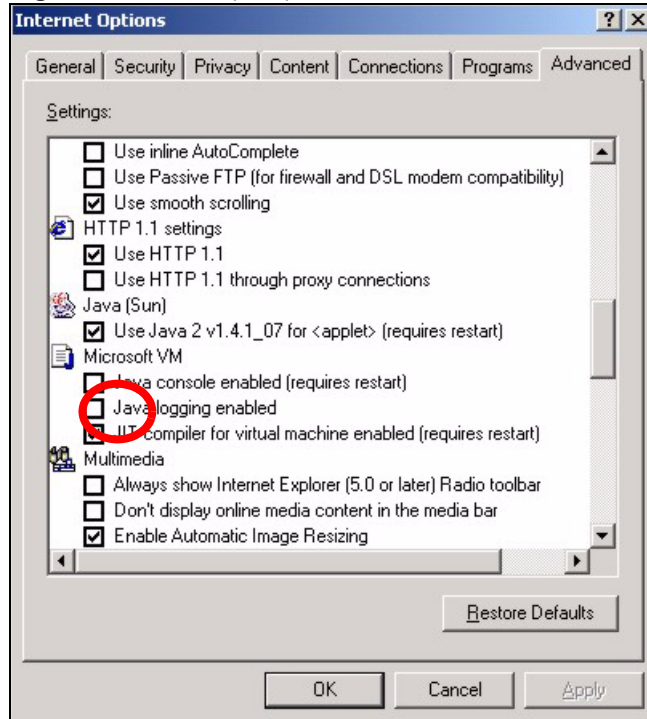
- 1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

**Figure 209** Security Settings - Java

#### 29.4.1.3.1 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 210 Java (Sun)



## 29.5 Telephone Problems

Table 140 Troubleshooting Telephone

PROBLEM	CORRECTIVE ACTION
The telephone port won't work or the telephone lacks a dial tone.	Check the telephone connections and telephone wire. Make sure you have the <b>VoIP SIP Settings</b> screen properly configured.
I can access the Internet, but cannot make VoIP calls.	Make sure you have the <b>VoIP SIP Settings</b> screen properly configured. One of the <b>PHONE</b> lights should come on. Make sure that your telephone is connected to the corresponding <b>PHONE</b> port. You can also check the VoIP status in the <b>Status</b> screen. If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.
I cannot call from one of the ZyXEL Device's phone ports to the other phone port.	You cannot call the SIP number of the SIP account that you are using to make a call. The ZyXEL Device generates a busy tone and does not attempt to establish a call if the SIP number you dial matches the outgoing SIP number of the phone port you are using. For example, if you set <b>Phone 1</b> to use SIP account 1 and set <b>Phone 2</b> to use SIP account 2, then you can use <b>Phone 1</b> to call to SIP account 2's SIP number or <b>Phone 2</b> to call to SIP account 1's SIP number.



# APPENDIX A

## Product Specifications

See also [Chapter 1 on page 41](#) for a general overview of the key features.

### Specification Tables

**Table 141** Device Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Server IP Pool	192.168.1.32 to 192.168.1.64
Static DHCP Addresses	10
Dimensions	(245 W) x (163 D) x (37 H) mm
Weight	605g
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
PHONE Ports	8 RJ-11 FXS POTS ports.
RESET Button	Restores factory defaults
Antenna	One attached external dipole antenna, 2dBi
Operation Temperature	0° C ~ 40° C
Storage Temperature	-30° ~ 60° C
Operation Humidity	20% ~ 95% RH
Storage Humidity	20% ~ 95% RH

### Firmware Specifications

**Table 142** Firmware Features

FEATURE	DESCRIPTION
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device.  <b>Note:</b> Only upload firmware for your specific model!

**Table 142** Firmware Features

FEATURE	DESCRIPTION
IEEE 802.11b/g Wireless LAN	The ZyXEL Device can serve as an IEEE 802.11g wireless access point. Expand your network by allowing IEEE 802.11g and IEEE 802.11b devices to connect to your network.
Wireless Security	The ZyXEL Device supports WEP encryption for basic security as well as WPA and WPA2 security standards.
MAC Address Filter	Allow or deny access to your wired or wireless network based on the MAC addresses of the computers communicating with your network.
Any IP	The Any IP feature allows a computer to access the Internet and the ZyXEL Device without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration and put it back on the ZyXEL Device later if you decide you want to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, <a href="http://www.zyxel.com">www.zyxel.com</a> for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP Alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the ZyXEL Device itself as the gateway for each subnet.
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the ZyXEL Device to an external UNIX syslog server.
PPPoE	PPPoE mimics a dial-up over Ethernet Internet access connection.
Universal Plug and Play (UPnP)	The ZyXEL Device can communicate with other UPnP enabled devices in a network.

**Table 142** Firmware Features

FEATURE	DESCRIPTION
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. The management server can securely manage and update configuration changes in ZyXEL Devices.
Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	Content filtering allows you to block access to Internet web sites that contain key words (that you specify) in the URL. You can also schedule when to perform the filtering and give trusted LAN IP addresses unfiltered Internet access.
Media Bandwidth Management	Media Bandwidth Management allows you to specify bandwidth classes based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth classes.
Auto Provisioning	Your VoIP service provider can automatically update your device's configuration via an auto-provisioning server.
IPSec VPN Capability	Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The ZyXEL Device VPN is based on the IPSec standard and is interoperable with other IPSec-based VPN products.

**Table 143** Firmware Specifications

ADSL Standards	<p>Support ITU G.992.1 G.dmt (Annex B, U-R2)  EOC specified in ITU-T G.992.1  ADSL2 G.dmt.bis (G.992.3)  ADSL2 G.lite.bis (G.992.4)  ADSL 2/2+ AnnexM  ADSL2+ (G.992.5)  Reach-Extended ADSL (RE ADSL)  SRA (Seamless Rate Adaptation)  Auto-negotiating rate adaptation  ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5)  Multi-protocol over AAL5 (RFC 2684/1483)  PPP over ATM AAL5 (RFC 2364)  PPP over Ethernet (RFC 2516)  Multiple PPPoE  VC-based and LLC-based multiplexing  Up to 8 PVCs (Permanent Virtual Circuits)  I.610 F4/F5 OAM  Zero configuration</p>
Other Protocol Support	<p>PPP (Point-to-Point Protocol) link layer protocol  Transparent bridging for unsupported network layer protocols  DHCP Server/Client/Relay  RIP I/RIP II  ICMP  ATM QoS  SNMP v1 and v2c with MIB II support (RFC 1213)  IP Multicasting IGMP v1 and v2  IGMP Proxy  UPnP</p>
Management	<p>Embedded Web Configurator  CLI (Command Line Interpreter)  SNMP v1 &amp; v2c with MIB II  Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore  Telnet for remote management  Remote Management Control: Telnet, FTP, Web, SNMP and DNS  VoIP Auto-provisioning via TFTP / HTTP / HTTPS  TR-069 Compliant  Remote Firmware Upgrade  Syslog</p>



**Table 143** Firmware Specifications (continued)

Wireless	<p>IEEE 802.11g Compliance  Frequency Range: 2.4 GHz ISM Band  Advanced Orthogonal Frequency Division Multiplexing (OFDM)  Data Rates: 54Mbps, 11Mbps, 5.5Mbps, 2Mbps, and 1 Mbps Auto Fallback  WPA/WPA2 security  WMM  IEEE 802.11i  IEEE 802.11e  Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit.  WLAN bridge to LAN  Up to 32 MAC Address filters  External RADIUS server using EAP-MD5, TLS, TTLS  Antenna: 2dBi, non-detachable</p>
Firewall	<p>Stateful Packet Inspection  Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc.  Access Control of Service  Content Filtering  IP &amp; Generic Packet Filtering  Real time Attack Alerts and Logs  Reports and logs  SIP ALG passthrough</p>
NAT/SUA	<p>Port Forwarding  2048 NAT sessions  Multimedia application  PPTP under NAT/SUA  IPSec passthrough  SIP ALG passthrough</p>
VPN	<p>20 Configurable IPSec tunnels  Maximum 2 simultaneous IPSec connections  IKE and Manual Key Management  AH and ESP Protocol  DES, 3DES and AES Encryption  SHA-1 and MD5 Authentication  Tunnel and Transport Mode Encapsulation  IPSec NAT Traversal  NETBIOS pass-through for IPSec</p>
Content Filtering	Web page blocking by URL keyword.
Static Routes	16 IP

**Table 143** Firmware Specifications (continued)

Voice Features	<p>SIP version 2 (Session Initiating Protocol RFC 3261)                  SDP (Session Description Protocol RFC 2327)                  RTP (RFC 1889)                  RTCP (RFC 1890)                  Voice codecs (coder/decoders) G.711, G.729                  G.168 echo cancellation (8ms ~ 16ms)                  Fax and data modem discrimination                  Silence Suppression / Voice Activity Detection (VAD)                  Comfort Noise Generation (CNG)                  Dynamic Jitter Buffer (Adaptive)                  DTMF Detection and Generation                  DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO)                  Point-to-point call establishment between two IADs                  Quick dialing through predefined phone book, which maps the phone dialing number and destination URL.                  Multiple SIP number registration and multiple signaling handling capability.(per POTS port)                  Caller ID support                  Flexible Dial Plan (RFC3525 section 7.1.14)                  Multiple SIP Accounts / Phone Numbers- Freely assignable Numbers to Each Phone Port (8 SIP accounts supported)                  PSTN Line allows you to make calls via your regular phone line even when the ZyXEL Device loses power.</p>
Other Features	<p>Any IP                  Zero Configuration (VC auto-hunting)                  Traffic Redirect                  Dynamic DNS                  IP Alias                  IP Policy Routing                  SPTGEN                  QoS</p>

## P-2608HW/HWL-Dx Series Power Adaptor Specifications

**Table 144** P-2608HW/HWL-Dx Series Power Adaptor Specifications

<b>DC MODEL PLUG STANDARDS</b>	
DC Power Adapter Model	NU40-2180200-I3
Input Power	AC 100~240V/50/60Hz, 1.2A
Output Power	DC 18Volts/2.0A
Power Consumption	22W
Safety Standards	UL, CUL (UL 60950 Third Edition, CSA C22.2 NO. 60950) ITS-GS, CE (EN 60950-1), (AS/NZS 60950: 2000)

# APPENDIX B

## Setting up Your Computer's IP Address

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

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

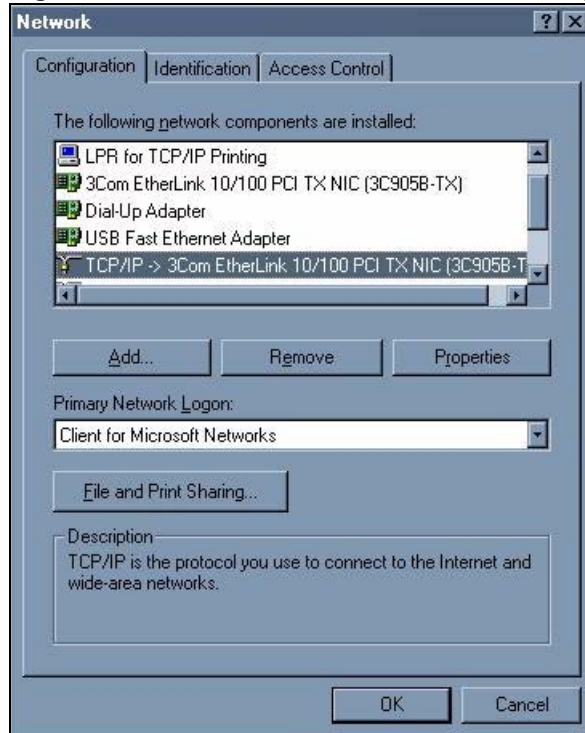
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

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

### Windows 95/98/Me

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

**Figure 211** 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:

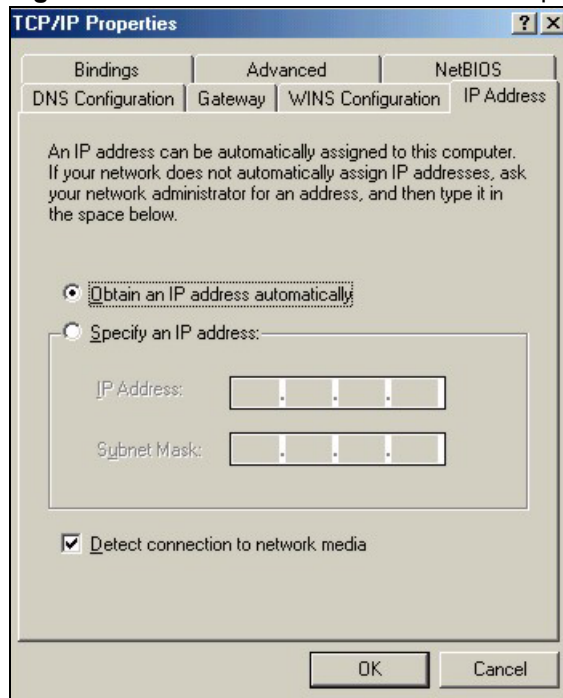
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

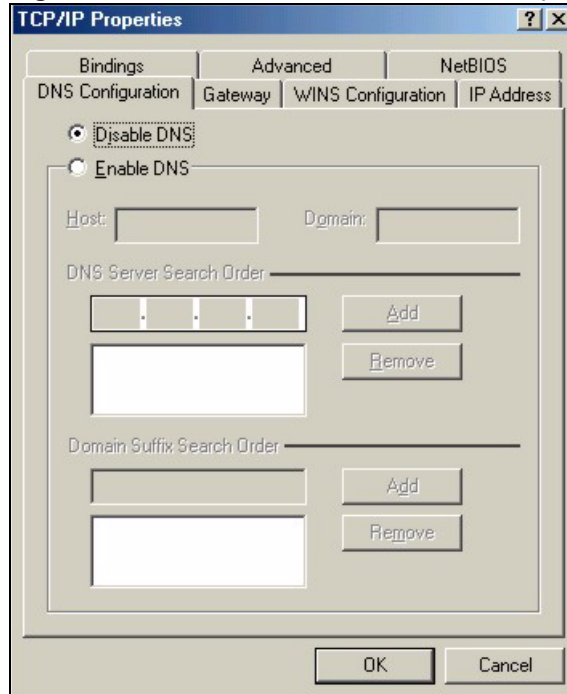
## Configuring

- 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 212** 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 213** Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

**5** Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Turn on your ZyXEL Device and restart your computer when prompted.

## Verifying Settings

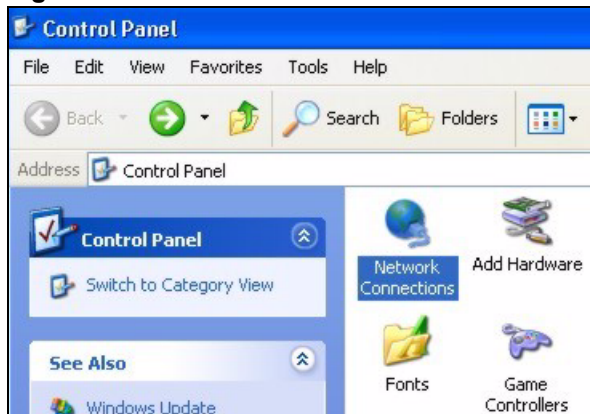
**1** Click **Start** and then **Run**.**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.**3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

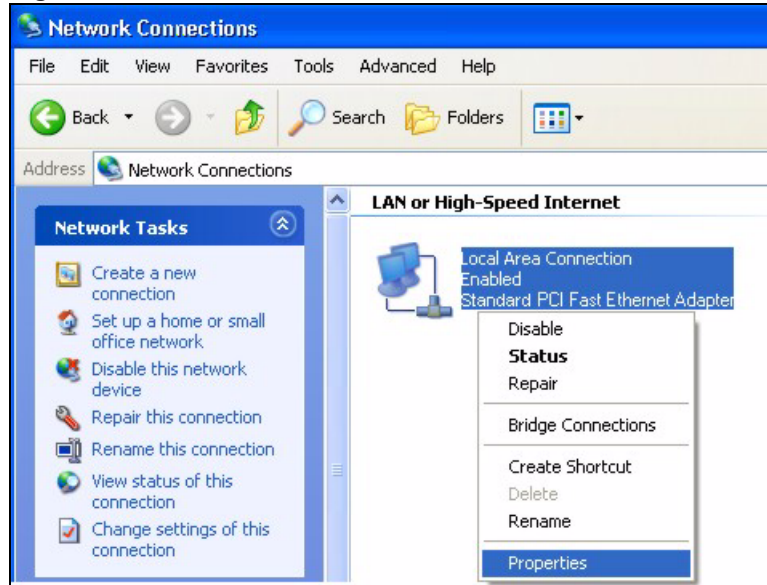
**1** For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

**Figure 214** Windows XP: Start Menu

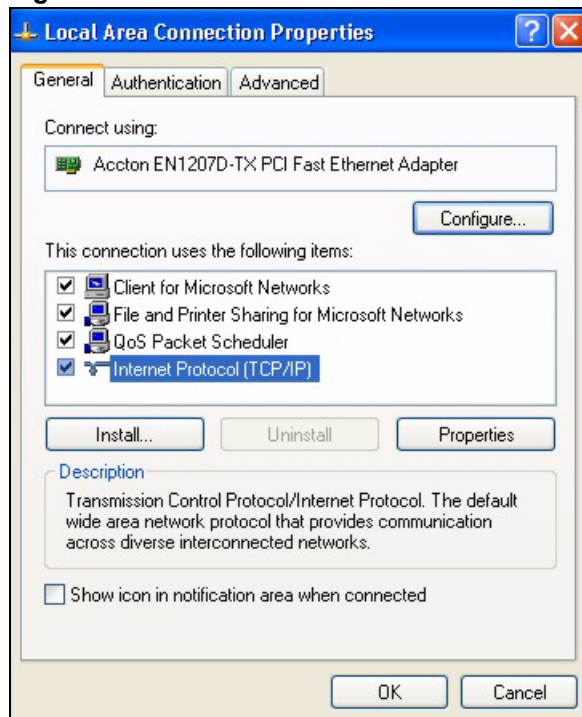
- 2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

**Figure 215** Windows XP: Control Panel

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

**Figure 216** Windows XP: Control Panel: Network Connections: Properties

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

**Figure 217** Windows XP: Local Area Connection Properties

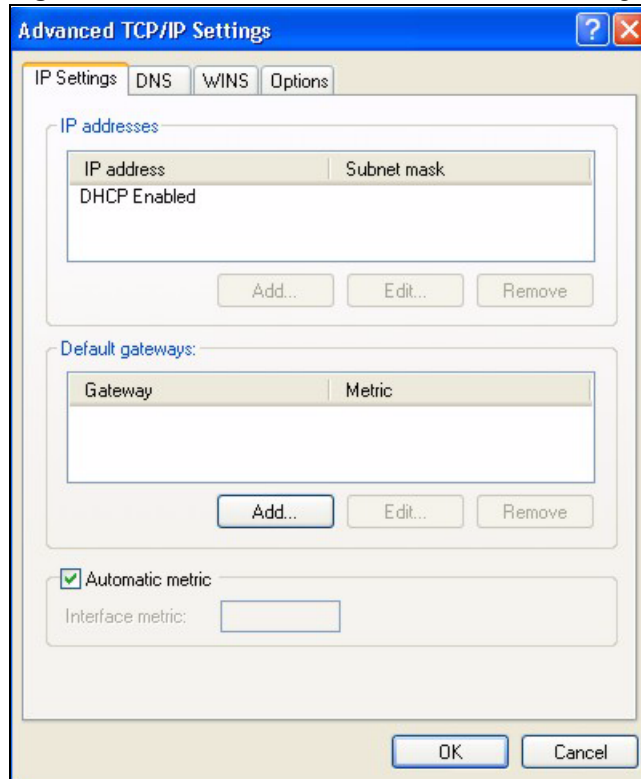
- 5** The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- 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 218** Windows XP: Advanced TCP/IP Settings



- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

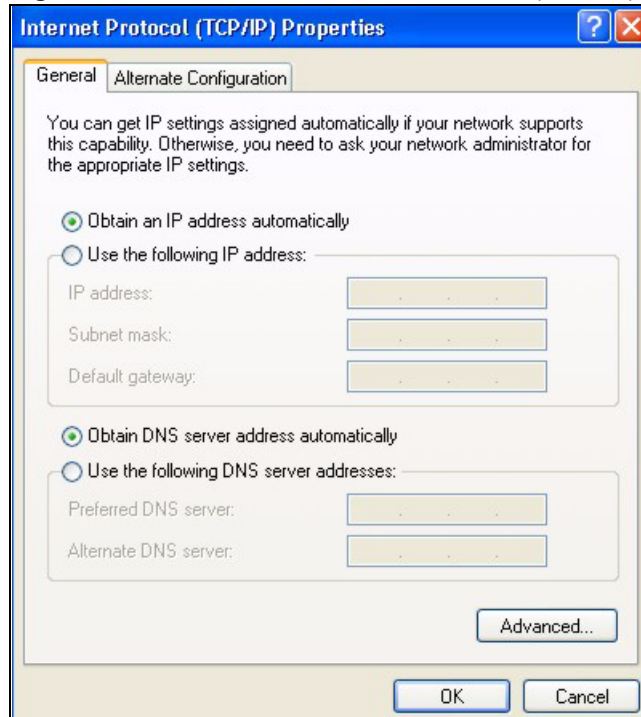
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

- 7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 219** Windows XP: Internet Protocol (TCP/IP) Properties



**8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

**9** Click **OK** to close the **Local Area Connection Properties** window.

**10** Turn on your ZyXEL Device and restart your computer (if prompted).

## Verifying Settings

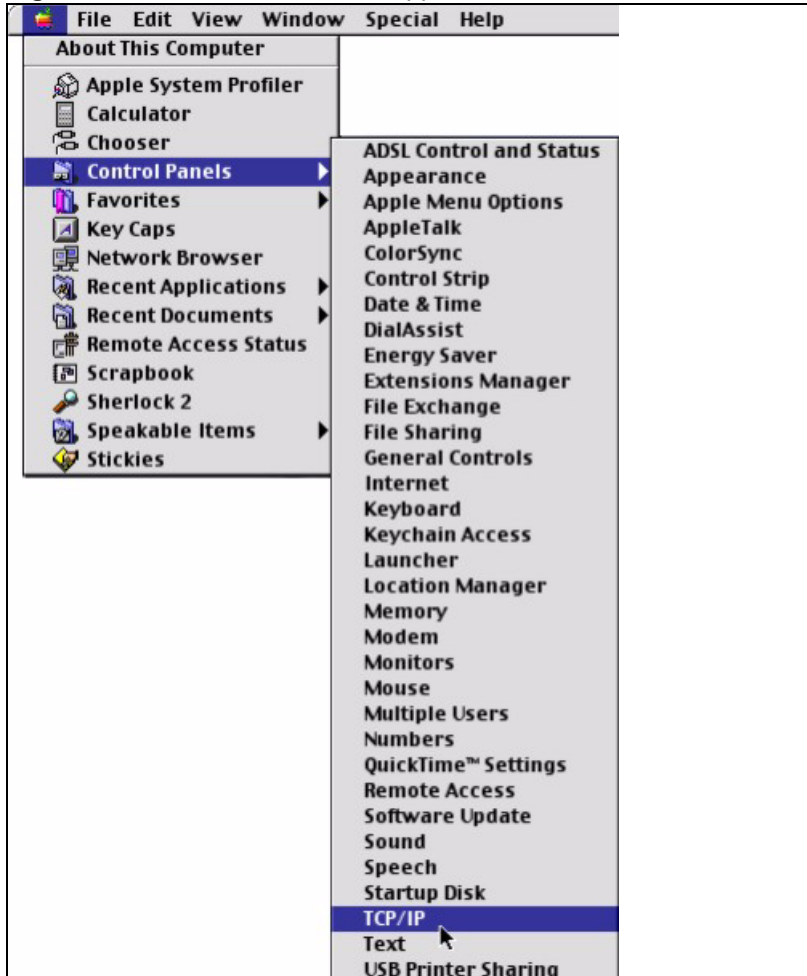
**1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

## Macintosh OS 8/9

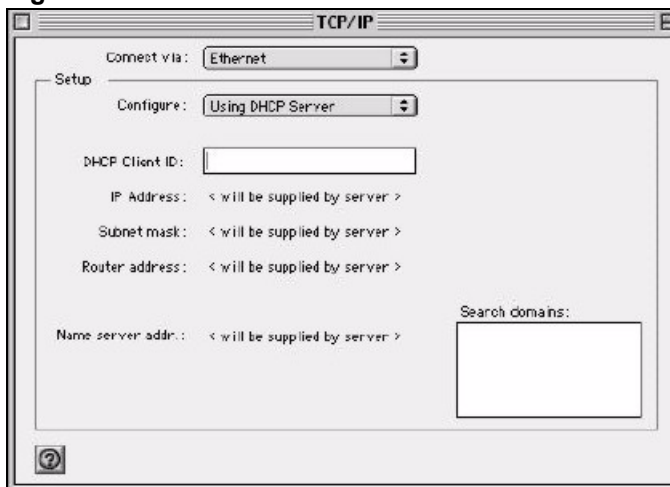
**1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 220 Macintosh OS 8/9: Apple Menu



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

Figure 221 Macintosh OS 8/9: TCP/IP



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

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

**5** Close the **TCP/IP Control Panel**.

**6** Click **Save** if prompted, to save changes to your configuration.

**7** Turn on your ZyXEL Device and restart your computer (if prompted).

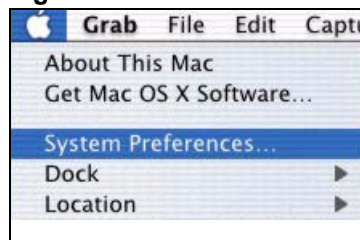
## Verifying Settings

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

## Macintosh OS X

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

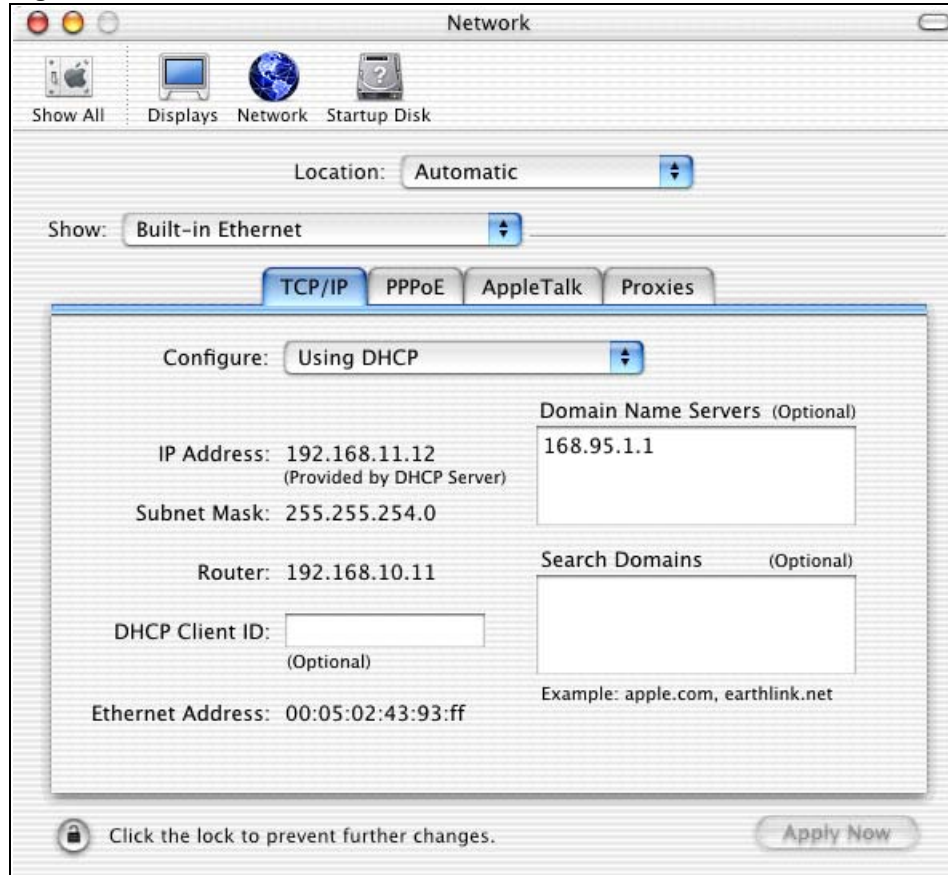
**Figure 222** Macintosh OS X: Apple Menu



**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 223** Macintosh OS X: Network

**4** For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

**5** Click **Apply Now** and close the window.

**6** Turn on your ZyXEL Device and restart your computer (if prompted).

## Verifying Settings

Check your TCP/IP properties in the **Network** window.



# APPENDIX C

## IP Addresses and Subnetting

This appendix introduces IP addresses, IP address classes and subnet masks. You use subnet masks to subdivide a network into smaller logical networks.

### Introduction to IP Addresses

An IP address has two parts: the network number and the host ID. Routers use the network number to send packets to the correct network, while the host ID identifies a single device on the network.

An IP address is made up of four octets, written in dotted decimal notation, for example, 192.168.1.1. (An octet is an 8-digit binary number. Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.)

There are several classes of IP addresses. The first network number (192 in the above example) defines the class of IP address. These are defined as follows:

- Class A: 0 to 127
- Class B: 128 to 191
- Class C: 192 to 223
- Class D: 224 to 239
- Class E: 240 to 255

### IP Address Classes and Hosts

The class of an IP address determines the number of hosts you can have on your network.

- In a class A address the first octet is the network number, and the remaining three octets are the host ID.
- In a class B address the first two octets make up the network number, and the two remaining octets make up the host ID.
- In a class C address the first three octets make up the network number, and the last octet is the host ID.

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

**Table 145** Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	<b>Network number</b>	Host ID	Host ID	Host ID
Class B	<b>Network number</b>	<b>Network number</b>	Host ID	Host ID
Class C	<b>Network number</b>	<b>Network number</b>	<b>Network number</b>	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have  $2^8 - 2$ , or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have  $2^{16} - 2$ , or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have  $2^{24} - 2$  hosts, or approximately 16 million hosts.

## IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an address.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

**Table 146** Allowed IP Address Range By Class

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



## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation).

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The “natural” masks for class A, B and C IP addresses are as follows.

**Table 147** “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

## Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits.

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

**Table 148** Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224

**Table 148** Alternative Subnet Mask Notation (continued)

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

## Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

**Table 149** Two Subnets Example

IP/SUBNET MASK	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C").

To make two networks, divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

**Note:** In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to make network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

**Table 150** Subnet 1

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

**Table 150** Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 151** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is  $2^7 - 2$  or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving  $2^6 - 2$  or 62 hosts for each subnet (all zeroes is the subnet itself, all ones is the broadcast address on the subnet).

**Table 152** Subnet 1

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

**Table 152** Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 153** Subnet 2

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

**Table 154** Subnet 3

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

**Table 155** Subnet 4

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

## Example Eight Subnets

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

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

**Table 156** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

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

**Table 157** Class C Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

## Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see [Table 145 on page 380](#)) available for subnetting.

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

**Table 158** Class B Subnet Planning

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

## Appendix D

# Common Services

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

**Table 159** Commonly Used Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.

**Table 159** Commonly Used Services

SERVICE	DESCRIPTION
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.



# APPENDIX E

## Importing Certificates

This appendix shows importing certificates examples using Internet Explorer 5.

### Import Prestige Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the Prestige's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

**Figure 224** Security Certificate



### Importing the Prestige's Certificate into Internet Explorer

For Internet Explorer to trust a self-signed certificate from the Prestige, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a Prestige certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the Prestige's (self-signed) server certificate into your operating system as a trusted certification authority.

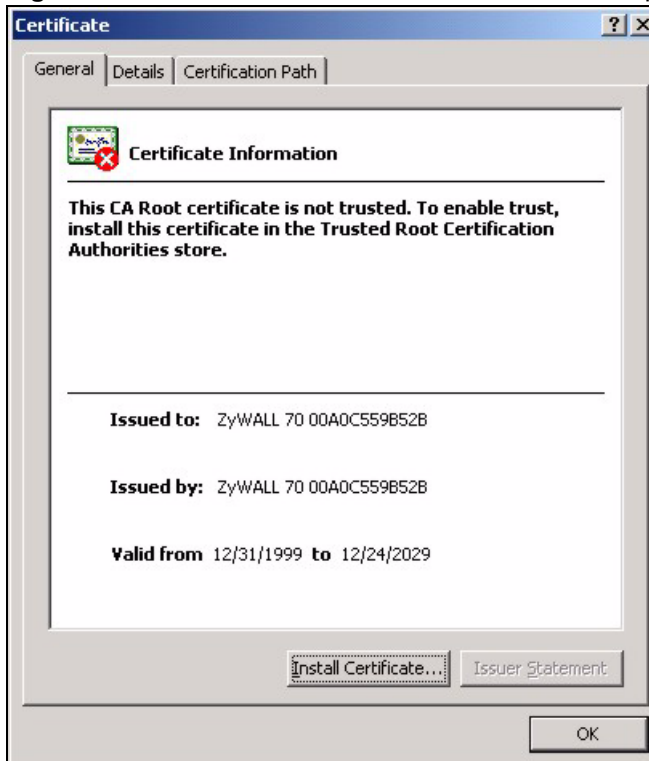
- 1 In Internet Explorer, double click the lock shown in the following screen.

**Figure 225** Login Screen



**2** Click **Install Certificate** to open the **Install Certificate** wizard.

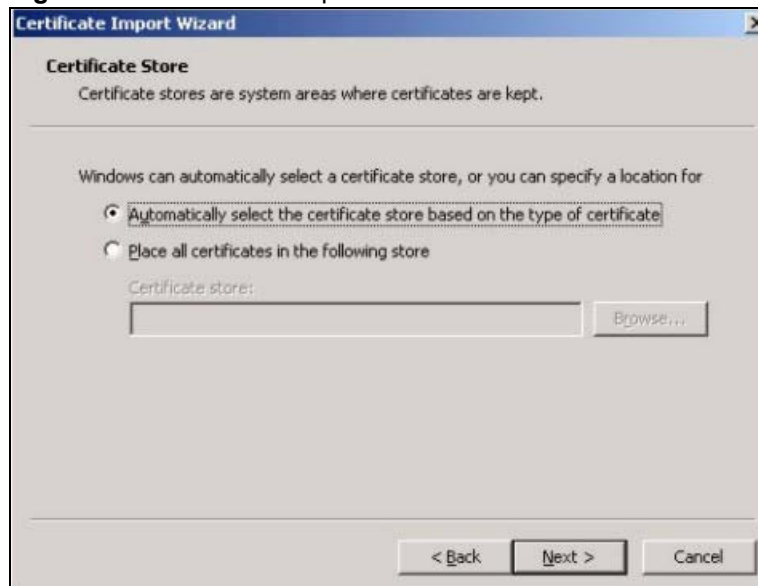
**Figure 226** Certificate General Information before Import



**3** Click **Next** to begin the **Install Certificate** wizard.

**Figure 227** Certificate Import Wizard 1

4 Select where you would like to store the certificate and then click **Next**.

**Figure 228** Certificate Import Wizard 2

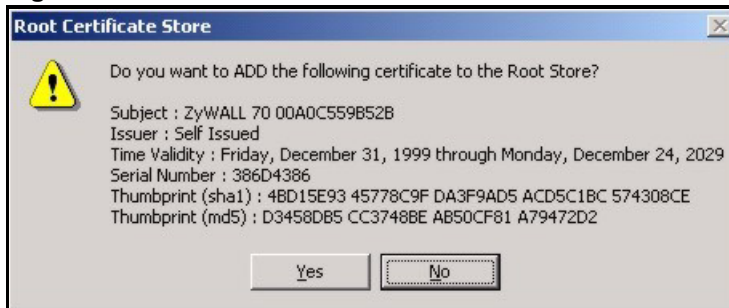
5 Click **Finish** to complete the **Import Certificate** wizard.

**Figure 229** Certificate Import Wizard 3



**6** Click **Yes** to add the Prestige certificate to the root store.

**Figure 230** Root Certificate Store



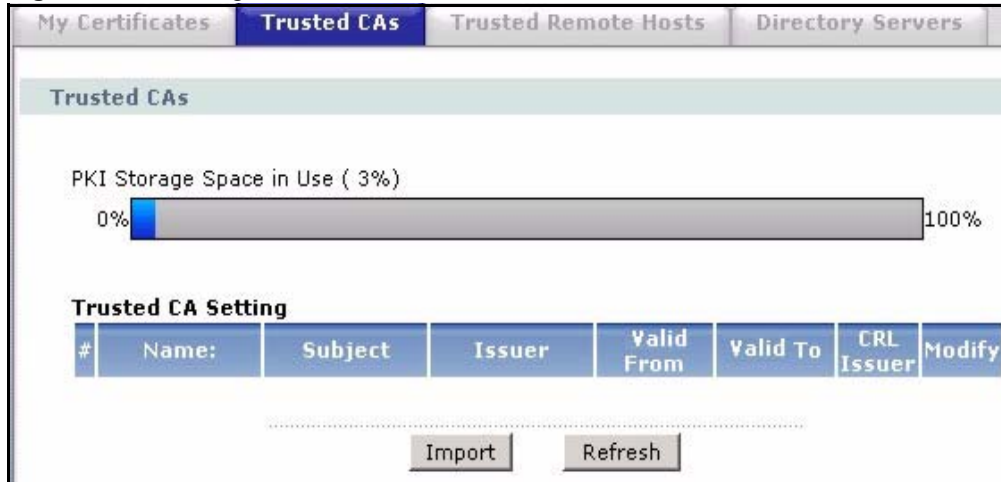
**Figure 231** Certificate General Information after Import

## Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the Prestige.

You must have imported at least one trusted CA to the Prestige in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the Prestige (see the Prestige's **Trusted CA** web configurator screen).

**Figure 232** Prestige Trusted CA Screen

The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

## Installing the CA's Certificate

- 1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

**Figure 233** CA Certificate Example

- 2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

## Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

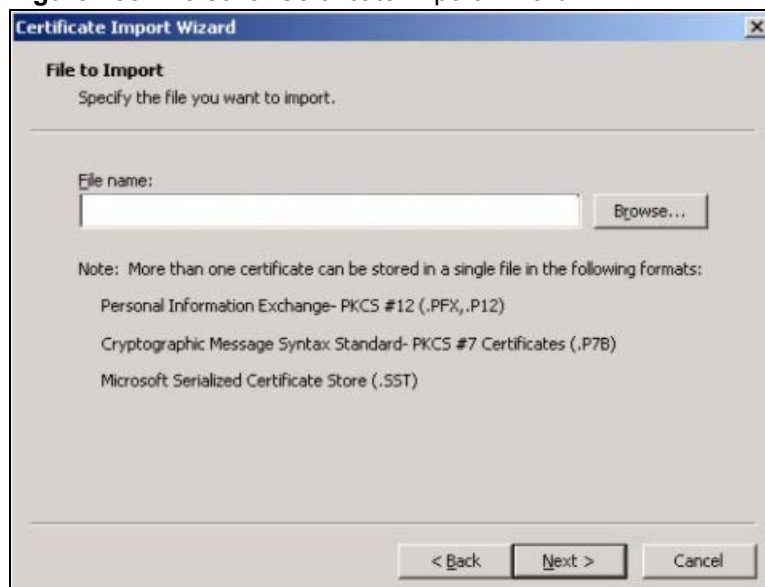
- 1 Click **Next** to begin the wizard.

**Figure 234** Personal Certificate Import Wizard 1



- 2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

**Figure 235** Personal Certificate Import Wizard 2



- 3 Enter the password given to you by the CA.

**Figure 236** Personal Certificate Import Wizard 3

The screenshot shows the 'Certificate Import Wizard' dialog box at the 'Password' step. The title bar reads 'Certificate Import Wizard'. The main text says 'To maintain security, the private key was protected with a password.' Below this, it asks the user to 'Type the password for the private key.' There is a text input field labeled 'Password:'. Two checkboxes are present: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' and 'Mark the private key as exportable'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

**Figure 237** Personal Certificate Import Wizard 4

The screenshot shows the 'Certificate Import Wizard' dialog box at the 'Certificate Store' step. The title bar reads 'Certificate Import Wizard'. The main text says 'Certificate stores are system areas where certificates are kept.' Below this, it says 'Windows can automatically select a certificate store, or you can specify a location for'. There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is selected) and 'Place all certificates in the following store'. Below the second option is a text input field labeled 'Certificate store:' with a 'Browse...' button to its right. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 5 Click **Finish** to complete the wizard and begin the import process.



**Figure 238** Personal Certificate Import Wizard 5

- 6** You should see the following screen when the certificate is correctly installed on your computer.

**Figure 239** Personal Certificate Import Wizard 6

## Using a Certificate When Accessing the Prestige Example

Use the following procedure to access the Prestige via HTTPS.

- 1** Enter 'https://Prestige IP Address/' in your browser's web address field.

**Figure 240** Access the Prestige Via HTTPS

- 2** When **Authenticate Client Certificates** is selected on the Prestige, the following screen asks you to select a personal certificate to send to the Prestige. This screen displays even if you only have a single certificate as in the example.

**Figure 241** SSL Client Authentication



**3** You next see the Prestige login screen.

**Figure 242** Prestige Secure Login Screen



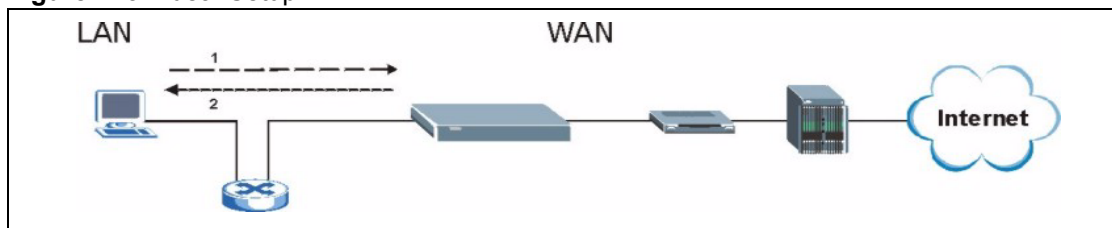
# APPENDIX F

## Triangle Route

### The Ideal Setup

When the firewall is on, your ZyXEL Device acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyXEL Device to protect your LAN against attacks.

**Figure 243** Ideal Setup

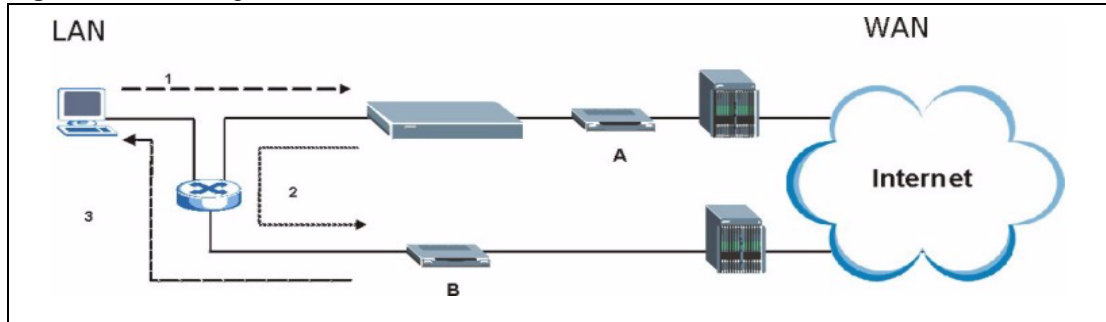


### The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

- 1** A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2** The ZyXEL Device reroutes the SYN packet through Gateway **B** on the LAN to the WAN.
- 3** The reply from the WAN goes directly to the computer on the LAN without going through the ZyXEL Device.

As a result, the ZyXEL Device resets the connection, as the connection has not been acknowledged.

**Figure 244** “Triangle Route” Problem

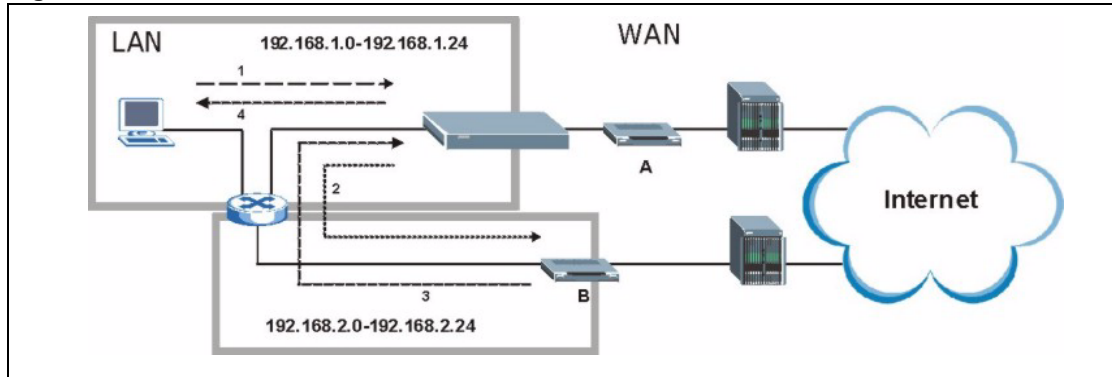
## The “Triangle Route” Solutions

This section presents you two solutions to the “triangle route” problem.

### IP Aliasing

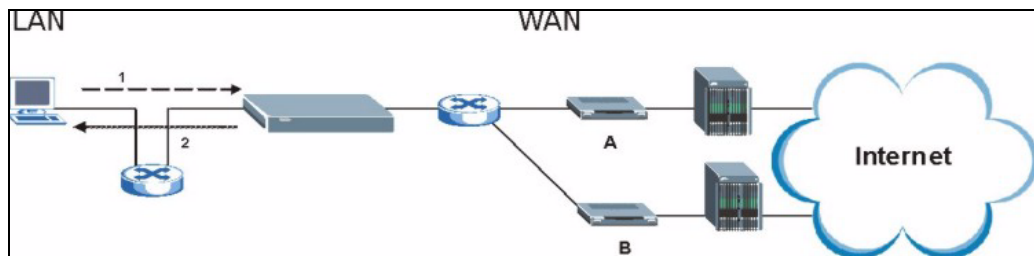
IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyXEL Device supports up to three logical LAN interfaces with the ZyXEL Device being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the ZyXEL Device to your LAN. The following steps describe such a scenario.

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

**Figure 245** IP Alias

## Gateways on the WAN Side

A second solution to the “triangle route” problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your ZyXEL Device to your LAN. Therefore your LAN is protected.

**Figure 246** Gateways on the WAN Side



# APPENDIX G

## Log Descriptions

This appendix provides descriptions of example log messages.

**Table 160** 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 160** 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 161** 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 162** 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 163** 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 <b>TCP Maximum Incomplete</b> in the <b>Firewall Attack Alerts</b> screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. Default timeout values: ICMP idle timeout (s): 60 UDP idle timeout (s): 60 TCP connection (three way handshaking) timeout (s): 30 TCP FIN-wait timeout (s): 60 TCP idle (established) timeout (s): 3600
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.) Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: "sys firewall tcprst").

**Table 164** Packet Filter Logs

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

For type and code details, see [Table 173 on page 409](#).

**Table 165** ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.

**Table 165** ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

**Table 166** 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 167** PPP Logs

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

**Table 168** UPnP Logs

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

**Table 169** Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: block keyword	The content of a requested web page matched a user defined keyword.
%s	The system forwarded web content.

For type and code details, see [Table 173 on page 409](#).

**Table 170** Attack Logs

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

**Table 170** Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.

**Table 171** 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication method.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.

**Table 171** 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

**Table 172** ACL Setting Notes

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

**Table 173** ICMP Notes

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

**Table 173** ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

**Table 174** Syslog Logs

LOG MESSAGE	DESCRIPTION
<pre>&lt;Facility*8 + Severity&gt;Mon dd hr:mm:ss hostname src="&lt;srcIP:srcPort&gt;" dst="&lt;dstIP:dstPort&gt;" msg="&lt;msg&gt;" note="&lt;note&gt;" devID="&lt;mac address last three numbers&gt;" cat="&lt;category&gt;"</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-&gt;LOGS-&gt;Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.</p>

**Table 175** SIP Logs

LOG MESSAGE	DESCRIPTION
SIP Registration Success by SIP:SIP Phone Number	The listed SIP account was successfully registered with a SIP register server.
SIP Registration Fail by SIP:SIP Phone Number	An attempt to register the listed SIP account with a SIP register server was not successful.
SIP UnRegistration Success by SIP:SIP Phone Number	The listed SIP account's registration was deleted from the SIP register server.
SIP UnRegistration Fail by SIP:SIP Phone Number	An attempt to delete the listed SIP account's registration from the SIP register server failed.

**Table 176** RTP Logs

LOG MESSAGE	DESCRIPTION
Error, RTP init fail	The initialization of an RTP session failed.
Error, Call fail: RTP connect fail	A VoIP phone call failed because the RTP session could not be established.
Error, RTP connection cannot close	The termination of an RTP session failed.

**Table 177** FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
VoIP Call Established Ph[Phone Port] -> Outgoing Call Number	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
VoIP Call End Phone[Phone Port]	A VoIP phone call made from a phone connected to the listed phone port has terminated.

**Table 178** FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start from SIP[SIP Port Number]	A VoIP phone call came to the ZyXEL Device from the listed SIP number.
VoIP Call Established Ph[Phone Port] <- Outgoing Call Number	A VoIP phone call was set up from the listed SIP number to the ZyXEL Device.
VoIP Call End Phone[Phone Port]	A VoIP phone call that came into the ZyXEL Device has terminated.

**Table 179** Lifeline Logs

LOG MESSAGE	DESCRIPTION
PSTN Call Start	A PSTN call has been initiated.
PSTN Call End	A PSTN call has terminated.
PSTN Call Established	A PSTN call has been set up.

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

**Table 180** RFC-2408 ISAKMP Payload Types

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

## Log Commands

Go to the command interpreter interface ([Appendix I on page 423](#) explains how to access and use the commands).

### Configuring What You Want the ZyXEL Device to Log

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

**Figure 247** Displaying Log Categories Example

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          ether          wan
wlan        ip            bridge        lan
radius      8021x         dsp           voiceradius   8021x
ras>
```

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



**Figure 248** Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both]
ras>
```

- 4 Use `sys logs category` followed by a log category and a parameter to decide what to record.

Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.

- 5 Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

## Displaying Logs

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

## Log Command Example

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

**Figure 249** Log Command Example

```

ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access
# .time                source                destination            notes
message
7|01/01/2000 09:40:13 |192.168.1.1:3        |192.168.1.33:1      |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
8|01/01/2000 09:40:07 |192.168.1.1:3        |192.168.1.33:1      |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
9|01/01/2000 09:40:04 |192.168.1.1:3        |192.168.1.33:1      |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
10|01/01/2000 09:40:04 |192.168.1.33:1199    |207.69.188.186:110  |ACCESS FO
RWARD
Firewall default policy: TCP (L to W)
11|01/01/2000 09:40:04 |192.168.1.1:53      |192.168.1.33:1200   |ACCESS FO
RWARD
none: UDP

```

# APPENDIX H

## Internal SPTGEN

### Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple ZyXEL Devices. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to navigate and configure individual screens for each ZyXEL Device.

### The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

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

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

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

**Figure 250** 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 250 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 251 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 250 on page 415](#)).

**Figure 251** 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 252** 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 253** Internal SPTGEN FTP Download Example

```

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

```

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

## Internal SPTGEN FTP Upload Example

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

**Figure 254** Internal SPTGEN FTP Upload Example

```

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

```

## Example Internal SPTGEN Screens

This section covers ZyXEL Device Internal SPTGEN screens.

**Table 181** Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number
FN	Field Name

**Table 181** Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the ZyXEL Device.

The following are the Internal SPTGEN menus.

**Table 182** 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 183** Menu 3

/ Menu 3.1 General Ethernet Setup			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1		= 2
30100002 =	Input Protocol filters Set 2		= 256
30100003 =	Input Protocol filters Set 3		= 256
30100004 =	Input Protocol filters Set 4		= 256
30100005 =	Input device filters Set 1		= 256
30100006 =	Input device filters Set 2		= 256
30100007 =	Input device filters Set 3		= 256
30100008 =	Input device filters Set 4		= 256
30100009 =	Output protocol filters Set 1		= 256
30100010 =	Output protocol filters Set 2		= 256
30100011 =	Output protocol filters Set 3		= 256
30100012 =	Output protocol filters Set 4		= 256
30100013 =	Output device filters Set 1		= 256
30100014 =	Output device filters Set 2		= 256
30100015 =	Output device filters Set 3		= 256
30100016 =	Output device filters Set 4		= 256
/ Menu 3.2 TCP/IP and DHCP Ethernet Setup			

**Table 183** Menu 3

FIN	FN	PVA	INPUT
30200001 =	DHCP	<0 (None)   1 (Server)   2 (Relay)>	= 0
30200002 =	Client IP Pool Starting Address		= 192.168.1.33
30200003 =	Size of Client IP Pool		= 32
30200004 =	Primary DNS Server		= 0.0.0.0
30200005 =	Secondary DNS Server		= 0.0.0.0
30200006 =	Remote DHCP Server		= 0.0.0.0
30200008 =	IP Address		= 172.21.2.200
30200009 =	IP Subnet Mask		= 16
30200010 =	RIP Direction	<0 (None)   1 (Both)   2 (In Only)   3 (Out Only)>	= 0
30200011 =	Version	<0 (Rip-1)   1 (Rip-2B)  2 (Rip-2M)>	= 0
30200012 =	Multicast	<0 (IGMP-v2)   1 (IGMP-v1)   2 (None)>	= 2
30200013 =	IP Policies Set 1 (1~12)		= 256
30200014 =	IP Policies Set 2 (1~12)		= 256
30200015 =	IP Policies Set 3 (1~12)		= 256
30200016 =	IP Policies Set 4 (1~12)		= 256
/ Menu 3.2.1 IP Alias Setup			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1	<0 (No)   1 (Yes)>	= 0
30201002 =	IP Address		= 0.0.0.0
30201003 =	IP Subnet Mask		= 0
30201004 =	RIP Direction	<0 (None)   1 (Both)   2 (In Only)   3 (Out Only)>	= 0
30201005 =	Version	<0 (Rip-1)   1 (Rip-2B)  2 (Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2		= 256

**Table 183** Menu 3

30201008 =	IP Alias #1 Incoming protocol filters Set 3		= 256	
30201009 =	IP Alias #1 Incoming protocol filters Set 4		= 256	
30201010 =	IP Alias #1 Outgoing protocol filters Set 1		= 256	
30201011 =	IP Alias #1 Outgoing protocol filters Set 2		= 256	
30201012 =	IP Alias #1 Outgoing protocol filters Set 3		= 256	
30201013 =	IP Alias #1 Outgoing protocol filters Set 4		= 256	
30201014 =	IP Alias 2 <0 (No)   1 (Yes)>		= 0	
30201015 =	IP Address		= 0.0.0.0	
30201016 =	IP Subnet Mask		= 0	
30201017 =	RIP Direction	<0 (None)   1 (Both)   2 (In Only)   3 (Out Only)>	= 0	
30201018 =	Version	<0 (Rip-1)   1 (Rip-2B)   2 (Rip-2M)>	= 0	
30201019 =	IP Alias #2 Incoming protocol filters Set 1		= 256	
30201020 =	IP Alias #2 Incoming protocol filters Set 2		= 256	
30201021 =	IP Alias #2 Incoming protocol filters Set 3		= 256	
30201022 =	IP Alias #2 Incoming protocol filters Set 4		= 256	
30201023 =	IP Alias #2 Outgoing protocol filters Set 1		= 256	
30201024 =	IP Alias #2 Outgoing protocol filters Set 2		= 256	
30201025 =	IP Alias #2 Outgoing protocol filters Set 3		= 256	
30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256	
*/ Menu 3.5 Wireless LAN Setup				
	FIN	FN	PVA	INPUT
30500001 =	ESSID			Wireless
30500002 =	Hide ESSID		<0 (No)   1 (Yes)>	= 0
30500003 =	Channel ID		<1 2 3 4 5 6 7 8 9 10 11 12 13>	= 1



**Table 183** Menu 3

30500004 =	RTS Threshold	<0 ~ 2432>	= 2432
30500005 =	FRAG. Threshold	<256 ~ 2432>	= 2432
30500006 =	WEP	<0 (DISABLE)   1 (64-bit WEP)   2 (128-bit WEP)>	= 0
30500007 =	Default Key	<1 2 3 4>	= 0
30500008 =	WEP Key1		=
30500009 =	WEP Key2		=
30500010 =	WEP Key3		=
30500011 =	WEP Key4		=
30500012 =	Wlan Active	<0 (Disable)   1 (Enable)>	= 0
*/ MENU 3.5.1 WLAN MAC ADDRESS FILTER			
FIN	FN	PVA	INPUT
30501001 =	Mac Filter Active	<0 (No)   1 (Yes)>	= 0
30501002 =	Filter Action	<0 (Allow)   1 (Deny)>	= 0
30501003 =	Address 1		= 00:00:00:00:0 0:00
30501004 =	Address 2		= 00:00:00:00:0 0:00
30501005 =	Address 3		= 00:00:00:00:0 0:00
Continued	...		...
30501034 =	Address 32		= 00:00:00:00:0 0:00

**Table 184** Menu 4 Internet Access Setup

/ Menu 4 Internet Access Setup			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0 (No)   1 (Yes)>	= 1
40000001 =	ISP	<0 (No)   1 (Yes)>	= 1

**Table 184** Menu 4 Internet Access Setup (continued)

40000002 =	Active	<0 (No)   1 (Yes)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2 (PPPOE)   3 (RFC 1483)   4 (PPPoA )   5 (ENET ENCAP)>	= 2
40000005 =	Multiplexing	<1 (LLC-based)   2 (VC-based)>	= 1
40000006 =	VPI #		= 0
40000007 =	VCI #		= 35
40000008 =	Service Name	<Str>	= any
40000009 =	My Login	<Str>	= test@pqa
40000010 =	My Password	<Str>	= 1234
40000011 =	Single User Account	<0 (No)   1 (Yes)>	= 1
40000012 =	IP Address Assignment	<0 (Static)   1 (D ynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0 (No)   1 (Yes)>	= 1
40000026 =	Bridge	<0 (No)   1 (Yes)>	= 0
40000027 =	ATM QoS Type	<0 (CBR)   (1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR)		= 0
40000029 =	Sustain Cell Rate (SCR)		= 0
40000030 =	Maximum Burst Size (MBS)		= 0
40000031 =	RIP Direction	<0 (None)   1 (Both)   2 (In Only)   3 (Out Only)>	= 0

**Table 184** Menu 4 Internet Access Setup (continued)

40000032=	RIP Version	<0 (Rip-1)   1 (Rip-2B)  2 (Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0 (No)  1 (Yes)>	= 0

**Table 185** Menu 12

/ Menu 12.1.1 IP Static Route Setup			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0 (No)  1 (Yes)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.2 IP Static Route Setup			
FIN	FN	PVA	INPUT
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0 (No)  1 (Yes)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask		= 0
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		= 0
120102007 =	IP Static Route set #2, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.3 IP Static Route Setup			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name	<Str>	=
120103002 =	IP Static Route set #3, Active	<0 (No)  1 (Yes)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0 (No)  1 (Yes)>	= 0

**Table 185** Menu 12 (continued)

/ Menu 12.1.4 IP Static Route Setup			
FIN	FN	PVA	INPUT
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0 (No)  1 (Yes)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0
120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.5 IP Static Route Setup			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0 (No)  1 (Yes)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0
120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.6 IP Static Route Setup			
FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0 (No)  1 (Yes)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.7 IP Static Route Setup			
FIN	FN	PVA	INPUT
120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0 (No)  1 (Yes)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0

**Table 185** Menu 12 (continued)

120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(No)  1(Yes)>	= 0
/ Menu 12.1.8 IP Static Route Setup			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name	<Str>	=
120108002 =	IP Static Route set #8, Active	<0(No)  1(Yes)>	= 0
120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0
120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0(No)  1(Yes)>	= 0
*/ Menu 12.1.9 IP Static Route Setup			
FIN	FN	PVA	INPUT
120109001 =	IP Static Route set #9, Name	<Str>	=
120109002 =	IP Static Route set #9, Active	<0(No)  1(Yes)>	= 0
120109003 =	IP Static Route set #9, Destination IP address		= 0.0.0.0
120109004 =	IP Static Route set #9, Destination IP subnetmask		= 0
120109005 =	IP Static Route set #9, Gateway		= 0.0.0.0
120109006 =	IP Static Route set #9, Metric		= 0
120109007 =	IP Static Route set #9, Private	<0(No)  1(Yes)>	= 0
*/ Menu 12.1.10 IP Static Route Setup			
FIN	FN	PVA	INPUT
120110001 =	IP Static Route set #10, Name		=
120110002 =	IP Static Route set #10, Active	<0(No)  1(Yes)>	= 0
120110003 =	IP Static Route set #10, Destination IP address		= 0.0.0.0
120110004 =	IP Static Route set #10, Destination IP subnetmask		= 0
120110005 =	IP Static Route set #10, Gateway		= 0.0.0.0
120110006 =	IP Static Route set #10, Metric		= 0
120110007 =	IP Static Route set #10, Private	<0(No)  1(Yes)>	= 0
*/ Menu 12.1.11 IP Static Route Setup			
FIN	FN	PVA	INPUT
120111001 =	IP Static Route set #11, Name	<Str>	=
120111002 =	IP Static Route set #11, Active	<0(No)  1(Yes)>	= 0
120111003 =	IP Static Route set #11, Destination IP address		= 0.0.0.0

**Table 185** Menu 12 (continued)

120111004 =	IP Static Route set #11, Destination IP subnetmask		= 0
120111005 =	IP Static Route set #11, Gateway		= 0.0.0.0
120111006 =	IP Static Route set #11, Metric		= 0
120111007 =	IP Static Route set #11, Private	<0 (No)  1 (Yes)>	= 0
*/ Menu 12.1.12 IP Static Route Setup			
FIN	FN	PVA	INPUT
120112001 =	IP Static Route set #12, Name	<Str>	=
120112002 =	IP Static Route set #12, Active	<0 (No)  1 (Yes)>	= 0
120112003 =	IP Static Route set #12, Destination IP address		= 0.0.0.0
120112004 =	IP Static Route set #12, Destination IP subnetmask		= 0
120112005 =	IP Static Route set #12, Gateway		= 0.0.0.0
120112006 =	IP Static Route set #12, Metric		= 0
120112007 =	IP Static Route set #12, Private	<0 (No)  1 (Yes)>	= 0
*/ Menu 12.1.13 IP Static Route Setup			
FIN	FN	PVA	INPUT
120113001 =	IP Static Route set #13, Name	<Str>	=
120113002 =	IP Static Route set #13, Active	<0 (No)  1 (Yes)>	= 0
120113003 =	IP Static Route set #13, Destination IP address		= 0.0.0.0
120113004 =	IP Static Route set #13, Destination IP subnetmask		= 0
120113005 =	IP Static Route set #13, Gateway		= 0.0.0.0
120113006 =	IP Static Route set #13, Metric		= 0
120113007 =	IP Static Route set #13, Private	<0 (No)  1 (Yes)>	= 0
*/ Menu 12.1.14 IP Static Route Setup			
FIN	FN	PVA	INPUT
120114001 =	IP Static Route set #14, Name	<Str>	=
120114002 =	IP Static Route set #14, Active	<0 (No)  1 (Yes)>	= 0
120114003 =	IP Static Route set #14, Destination IP address		= 0.0.0.0
120114004 =	IP Static Route set #14, Destination IP subnetmask		= 0
120114005 =	IP Static Route set #14, Gateway		= 0.0.0.0
120114006 =	IP Static Route set #14, Metric		= 0
120114007 =	IP Static Route set #14, Private	<0 (No)  1 (Yes)>	= 0
*/ Menu 12.1.15 IP Static Route Setup			
FIN	FN	PVA	INPUT
120115001 =	IP Static Route set #15, Name	<Str>	=

**Table 185** Menu 12 (continued)

120115002 =	IP Static Route set #15, Active	<0 (No)   1 (Yes)>	= 0
120115003 =	IP Static Route set #15, Destination IP address		= 0.0.0.0
120115004 =	IP Static Route set #15, Destination IP subnetmask		= 0
120115005 =	IP Static Route set #15, Gateway		= 0.0.0.0
120115006 =	IP Static Route set #15, Metric		= 0
120115007 =	IP Static Route set #15, Private	<0 (No)   1 (Yes)>	= 0
*/ Menu 12.1.16 IP Static Route Setup			
FIN	FN	PVA	INPUT
120116001 =	IP Static Route set #16, Name	<Str>	=
120116002 =	IP Static Route set #16, Active	<0 (No)   1 (Yes)>	= 0
120116003 =	IP Static Route set #16, Destination IP address		= 0.0.0.0
120116004 =	IP Static Route set #16, Destination IP subnetmask		= 0
120116005 =	IP Static Route set #16, Gateway		= 0.0.0.0
120116006 =	IP Static Route set #16, Metric		= 0
120116007 =	IP Static Route set #16, Private	<0 (No)   1 (Yes)>	= 0

**Table 186** Menu 15 SUA Server Setup

/ Menu 15 SUA Server Setup			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Active	<0 (No)   1 (Yes)>	= 0
150000003 =	SUA Server #2 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000004 =	SUA Server #2 Port Start		= 0
150000005 =	SUA Server #2 Port End		= 0
150000006 =	SUA Server #2 Local IP address		= 0.0.0.0
150000007 =	SUA Server #3 Active	<0 (No)   1 (Yes)>	= 0
150000008 =	SUA Server #3 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000009 =	SUA Server #3 Port Start		= 0
150000010 =	SUA Server #3 Port End		= 0
150000011 =	SUA Server #3 Local IP address		= 0.0.0.0
150000012 =	SUA Server #4 Active	<0 (No)   1 (Yes)>	= 0
150000013 =	SUA Server #4 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0

**Table 186** Menu 15 SUA Server Setup (continued)

150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0 (No)   1 (Yes)>	= 0
150000018 =	SUA Server #5 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000019 =	SUA Server #5 Port Start		= 0
150000020 =	SUA Server #5 Port End		= 0
150000021 =	SUA Server #5 Local IP address		= 0.0.0.0
150000022 =	SUA Server #6 Active	<0 (No)   1 (Yes)> = 0	= 0
150000023 =	SUA Server #6 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000024 =	SUA Server #6 Port Start		= 0
150000025 =	SUA Server #6 Port End		= 0
150000026 =	SUA Server #6 Local IP address		= 0.0.0.0
150000027 =	SUA Server #7 Active	<0 (No)   1 (Yes)>	= 0
150000028 =	SUA Server #7 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0
150000031 =	SUA Server #7 Local IP address		= 0.0.0.0
150000032 =	SUA Server #8 Active	<0 (No)   1 (Yes)>	= 0
150000033 =	SUA Server #8 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000034 =	SUA Server #8 Port Start		= 0
150000035 =	SUA Server #8 Port End		= 0
150000036 =	SUA Server #8 Local IP address		= 0.0.0.0
150000037 =	SUA Server #9 Active	<0 (No)   1 (Yes)>	= 0
150000038 =	SUA Server #9 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000039 =	SUA Server #9 Port Start		= 0
150000040 =	SUA Server #9 Port End		= 0
150000041 =	SUA Server #9 Local IP address		= 0.0.0.0
150000042 =	SUA Server #10 Active	<0 (No)   1 (Yes)>	= 0
150000043 =	SUA Server #10 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000044 =	SUA Server #10 Port Start		= 0
150000045 =	SUA Server #10 Port End		= 0
150000046 =	SUA Server #10 Local IP address		= 0.0.0.0
150000047 =	SUA Server #11 Active	<0 (No)   1 (Yes)>	= 0



**Table 186** Menu 15 SUA Server Setup (continued)

150000048 =	SUA Server #11 Protocol	<0 (All)   6 (TCP)   17 (UDP) >	= 0
150000049 =	SUA Server #11 Port Start		= 0
150000050 =	SUA Server #11 Port End		= 0
150000051 =	SUA Server #11 Local IP address		= 0.0.0.0
150000052 =	SUA Server #12 Active	<0 (No)   1 (Yes) >	= 0
150000053 =	SUA Server #12 Protocol	<0 (All)   6 (TCP)   17 (UDP) >	= 0
150000054 =	SUA Server #12 Port Start		= 0
150000055 =	SUA Server #12 Port End		= 0
150000056 =	SUA Server #12 Local IP address		= 0.0.0.0

**Table 187** Menu 21.1 Filter Set #1

/ Menu 21 Filter set #1			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=
/ Menu 21.1.1.1 set #1, rule #1			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1,Rule 1 Type	<2 (TCP/IP) >	= 2
210101002 =	IP Filter Set 1,Rule 1 Active	<0 (No)   1 (Yes) >	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address		= 0.0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask		= 0
210101006 =	IP Filter Set 1,Rule 1 Dest Port		= 137
210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match	<1 (check next)   2 (forward)   3 (drop) >	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match	<1 (check next)   2 (forward)   3 (drop) >	= 1

**Table 187** Menu 21.1 Filter Set #1 (continued)

/ Menu 21.1.1.2 set #1, rule #2			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type	<2 (TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0 (No)  1 (Yes)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210102008 =	IP Filter Set 1,Rule 2 Src IP address		= 0.0.0.0
210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port		= 0
210102011 =	IP Filter Set 1,Rule 2 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 1
/ Menu 21.1.1.3 set #1, rule #3			
FIN	FN	PVA	INPUT
210103001 =	IP Filter Set 1,Rule 3 Type	<2 (TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active	<0 (No)  1 (Yes)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port		= 139
210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address		= 0.0.0.0
210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0

**Table 187** Menu 21.1 Filter Set #1 (continued)

210103013 =	IP Filter Set 1,Rule 3 Act Match	<1 (check next)  2 (forward)   3 (drop)	= 3
210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1 (check next)  2 (forward)   3 (drop)	= 1
/ Menu 21.1.1.4 set #1, rule #4			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type	<2 (TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0 (No)  1 (Yes)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1 (check next)  2 ( forward)   3 (drop)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1 (check next)  2 (forward)   3 (drop)	= 1
/ Menu 21.1.1.5 set #1, rule #5			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type	<2 (TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active	<0 (No)  1 (Yes)>	= 1
210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0

**Table 187** Menu 21.1 Filter Set #1 (continued)

210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match	<1 (Check Next)  2 (Forward)  3 (Drop)>	= 1
/ Menu 21.1.1.6 set #1, rule #6			
FIN	FN	PVA	INPUT
210106001 =	IP Filter Set 1,Rule 6 Type	<2 (TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0 (No)  1 (Yes)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139
210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210106013 =	IP Filter Set 1,Rule 6 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 2

**Table 188** Menu 21.1 Filer Set #2,

/ Menu 21.1 filter set #2,			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN

**Table 188** Menu 21.1 Filer Set #2, (continued)

/ Menu 21.1.2.1 Filter set #2, rule #1			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2, Rule 1 Type	<0 (none)   2 (TCP/IP)>	= 2
210201002 =	IP Filter Set 2, Rule 1 Active	<0 (No)   1 (Yes)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port		= 137
210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater)>	= 1
210201008 =	IP Filter Set 2, Rule 1 Src IP address		= 0.0.0.0
210201009 =	IP Filter Set 2, Rule 1 Src Subnet Mask		= 0
210201010 =	IP Filter Set 2, Rule 1 Src Port		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match	<1 (check next)   2 (forward)   3 (drop)>	= 3
210201014 =	IP Filter Set 2, Rule 1 Act Not Match	<1 (check next)   2 (forward)   3 (drop)>	= 1
/ Menu 21.1.2.2 Filter set #2, rule #2			
FIN	FN	PVA	INPUT
210202001 =	IP Filter Set 2, Rule 2 Type	<0 (none)   2 (TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active	<0 (No)   1 (Yes)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address		= 0.0.0.0

**Table 188** Menu 21.1 Filer Set #2, (continued)

210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask		= 0
210202010 =	IP Filter Set 2, Rule 2 Src Port		= 0
210202011 =	IP Filter Set 2, Rule 2 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210202014 =	IP Filter Set 2, Rule 2 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 1
/ Menu 21.1.2.3 Filter set #2, rule #3			
FIN	FN	PVA	INPUT
210203001 =	IP Filter Set 2, Rule 3 Type	<0 (none)  2 (TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active	<0 (No)  1 (Yes)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask		= 0
210203006 =	IP Filter Set 2, Rule 3 Dest Port		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address		= 0.0.0.0
210203009 =	IP Filter Set 2, Rule 3 Src Subnet Mask		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port		= 0
210203011 =	IP Filter Set 2, Rule 3 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210203013 =	IP Filter Set 2, Rule 3 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210203014 =	IP Filter Set 2, Rule 3 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 1
/ Menu 21.1.2.4 Filter set #2, rule #4			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type	<0 (none)  2 (TCP/IP)>	= 2

**Table 188** Menu 21.1 Filer Set #2, (continued)

210204002 =	IP Filter Set 2, Rule 4 Active		<0 (No)   1 (Yes) > = 1
210204003 =	IP Filter Set 2, Rule 4 Protocol		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address		= 0.0.0.0
210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port		= 137
210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 0
210204013 =	IP Filter Set 2, Rule 4 Act Match	<1 (check next)   2 (forward)   3 (drop) >	= 3
210204014 =	IP Filter Set 2, Rule 4 Act Not Match	<1 (check next)   2 (forward)   3 (drop) >	= 1
/ Menu 21.1.2.5 Filter set #2, rule #5			
FIN	FN	PVA	INPUT
210205001 =	IP Filter Set 2, Rule 5 Type	<0 (none)   2 (TCP/IP) >	= 2
210205002 =	IP Filter Set 2, Rule 5 Active	<0 (No)   1 (Yes) >	= 1
210205003 =	IP Filter Set 2, Rule 5 Protocol		= 17
210205004 =	IP Filter Set 2, Rule 5 Dest IP address		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port		= 0

**Table 188** Menu 21.1 Filer Set #2, (continued)

210205011 =	IP Filter Set 2, Rule 5 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210205014 =	IP Filter Set 2, Rule 5 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 1
/ Menu 21.1.2.6 Filter set #2, rule #6			
FIN	FN	PVA	INPUT
210206001 =	IP Filter Set 2, Rule 6 Type	<0 (none)  2 (TCP/IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active	<0 (No)  1 (Yes)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol		= 17
210206004 =	IP Filter Set 2, Rule 6 Dest IP address		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210206013 =	IP Filter Set 2, Rule 6 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210206014 =	IP Filter Set 2, Rule 6 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 2
241100005 =	FTP Server Access	<0 (all)  1 (none)  2 (LAN)  3 (Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0 (all)  1 (none)  2 (LAN)  3 (Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0



**Table 189** Menu 23 System Menus

*/ Menu 23.1 System Password Setup			
FIN	FN	PVA	INPUT
230000000 =	System Password		= 1234
*/ Menu 23.2 System security: radius server			
FIN	FN	PVA	INPUT
230200001 =	Authentication Server Configured	<0 (No)   1 (Yes)>	= 1
230200002 =	Authentication Server Active	<0 (No)   1 (Yes)>	= 1
230200003 =	Authentication Server IP Address		= 192.168.1.32
230200004 =	Authentication Server Port		= 1822
230200005 =	Authentication Server Shared Secret		= 111111111111 111 111111111111 1111
230200006 =	Accounting Server Configured	<0 (No)   1 (Yes)>	= 1
230200007 =	Accounting Server Active	<0 (No)   1 (Yes)>	= 1
230200008 =	Accounting Server IP Address		= 192.168.1.44
230200009 =	Accounting Server Port		= 1823
230200010 =	Accounting Server Shared Secret		= 1234
*/ Menu 23.4 System security: IEEE802.1x			
FIN	FN	PVA	INPUT
230400001 =	Wireless Port Control	<0 (Authentication Required)   1 (No Access Allowed)   2 (No Authentication Required)>	= 2
230400002 =	ReAuthentication Timer (in second)		= 555
230400003 =	Idle Timeout (in second)		= 999
230400004 =	Authentication Databases	<0 (Local User Database Only)   1 (RADIUS Only)   2 (Local, RADIUS)   3 (RADIUS, Local)>	= 1
230400005 =	Key Management Protocol	<0 (8021x)   1 (WPA)   2 (WPAPSK)>	= 0
230400006 =	Dynamic WEP Key Exchange	<0 (Disable)   1 (64-bit WEP)   2 (128-bit WEP)>	= 0
230400007 =	PSK =		=

**Table 189** Menu 23 System Menus (continued)

230400008 =	WPA Mixed Mode	<0 (Disable)   1 (Enable)>	= 0
230400009 =	Data Privacy for Broadcast/Multicast packets	<0 (TKIP)   1 (WEP)>	= 0
230400010 =	WPA Broadcast/Multicast Key Update Timer		= 0

**Table 190** Menu 24.11 Remote Management Control

/ Menu 24.11 Remote Management Control			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port		= 23
241100002 =	TELNET Server Access	<0 (all)   1 (none)   2 (LAN)   3 (Wan)>	= 0
241100003 =	TELNET Server Secured IP address		= 0.0.0.0
241100004 =	FTP Server Port		= 21
241100005 =	FTP Server Access	<0 (all)   1 (none)   2 (LAN)   3 (Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0 (all)   1 (none)   2 (LAN)   3 (Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

## Command Examples

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

**Table 191** Command Examples

FIN	FN	PVA	INPUT
/ci command (for annex a): wan adsl opencmd			
990000001 =	ADSL OPMD	<0 (glite)   1 (t1.413)   2 (gdm)   3 (multimode)>	= 3
/ci command (for annex B): wan adsl opencmd			

**Table 191** Command Examples (continued)

	<b>FIN</b>	<b>FN</b>	<b>PVA</b>	<b>INPUT</b>
	FIN	FN	PVA	INPUT
	990000001 =	ADSL OPMD	<0(etsi) 1(normal)  2(gdmt) 3(multimo de)>	= 3



# Index

## A

AAL5 [364](#)  
 AbS [156](#)  
 active protocol [228](#)  
   AH [228](#)  
   and encapsulation [228](#)  
   ESP [228](#)  
 Address Resolution Protocol (ARP) [110](#)  
 administrator  
   password [320](#)  
 ADSL2 [364](#)  
 AH [228](#)  
   and transport mode [229](#)  
 alerts [326](#)  
 alerts, and firewall [202](#)  
 alerts, types of logs [325](#)  
 ALG [149](#)  
 alternative subnet mask notation [381](#)  
 Analysis-by-Synthesis, codec [156](#)  
 Antenna [361](#)  
 anti-probing  
   ICMP [303](#)  
 any IP [109](#)  
   and NAT [110](#)  
   example [110](#)  
   how it works [110](#)  
   setup [112](#)  
 application  
   UPnP [307](#)  
 application based bandwidth management [278](#)  
 Application Layer Gateway [149](#), [155](#)  
 application priority configuration [136](#)  
 application-level firewalls [188](#)  
 applications  
   static route [274](#)  
 ATM AAL5 [364](#)  
 ATM Adaptation Layer 5 (AAL5) [90](#)  
 ATM Adaptation Layer type 5 [364](#)  
 attack alert [215](#)  
 attack types, and firewalls [192](#)  
 authentication algorithms [223](#)  
   and active protocol [223](#)  
 Authentication Header. See AH.  
 automatic log out [47](#)  
 Auto-negotiating Rate Adaptation [364](#)

## B

backup configuration [335](#)  
 backup gateway [102](#), [104](#)  
 backup type [104](#)  
 bandwidth management [277](#), [279](#), [281](#)  
   allocating [277](#)  
   and rules [283](#)  
   capacity [277](#)  
   classes [279](#)  
   configuration [282](#)  
   example [278](#)  
   limits [277](#)  
   maximizing [279](#)  
   maximizing example [280](#)  
   monitor [287](#)  
   predefined services [73](#)  
   priority based [278](#)  
   schedule [278](#)  
   summary [282](#)  
   types [277](#)  
   types of priorities [281](#)  
 bandwidth management, wizard [73](#)  
 basic wireless security [63](#)  
 blocking keywords [217](#)  
 blocking time, and firewall [214](#)  
 browser, recommended settings [351](#)  
 brute-force attack, and firewalls [191](#)

## C

CA (Certification Authority) [249](#)  
 call forwarding [179](#)  
 call hold [168](#), [170](#)  
 call policy [179](#)  
 call service mode [168](#), [170](#)  
 call transfer [169](#), [170](#)  
 call waiting [169](#), [170](#)  
 Caller ID [366](#)  
 CBR (Continuous Bit Rate) [98](#)  
 certificate  
   details [256](#)  
   factory default [251](#)  
 certificates [249](#)  
   advantages [250](#)

- and cryptology [249](#)
- and directory servers [250](#), [270](#)
- and IKE SA [225](#)
- and public-key cryptology [249](#)
- and public-private keys [249](#)
- and remote hosts [264](#)
- and remote management [294](#)
- creating [254](#)
- file formats [253](#)
- generating requests [249](#)
- importing [253](#)
- remote hosts [267](#)
- replacing [251](#)
- revoked [250](#)
- storage space [251](#)
- trusted CAs [259](#), [261](#)
- verifying [266](#)

Certification Authority (CA) [249](#)

certifications [4](#)

- notices [5](#)
- viewing [5](#)

change password

- at login [46](#)

channel ID [124](#)

circuit-switched telephone networks [151](#)

Class of Service [158](#)

Class of Service (CoS) [158](#)

classes, and bandwidth management [280](#)

client server, SIP [152](#)

client-server protocol [152](#)

CNG [366](#)

codec [156](#)

codec, Analysis-by-Synthesis [156](#)

codec, waveform [156](#)

Codecs [366](#)

coder/decoder [156](#)

Comfort Noise Generation [366](#)

conference calls [169](#)

configuration file

- and FTP [340](#)
- and WAN [332](#)
- backup [335](#)
- naming conventions [331](#)

configuration files [331](#)

connections, hardware [349](#)

console port

- and remote management [293](#)

contact information [9](#)

content filtering [217](#)

- categories [217](#)
- configuration [217](#)
- schedule [218](#)
- trusted computers [219](#)
- URL keyword blocking [217](#)

- copyright [3](#)
- CoS [158](#)
- cost of transmission [92](#)
- creating certificates [254](#)
- custom ports
  - creating/editing [209](#)
- custom ports, and firewalls [208](#)
- custom services, and firewalls [208](#)
- customer support [9](#)

## D

daylight saving [321](#)

decoder [156](#)

default LAN IP address [45](#)

default settings [331](#), [336](#)

Denial of Service (DoS) [189](#), [214](#)

denial of service, attacks [188](#)

destination address, and firewalls [201](#)

DHCP [106](#), [107](#)

- and dynamic DNS [289](#)
- domain name [319](#)

DHCP server [113](#)

diagnostics [345](#)

- connection status [346](#)
- DSL line test [345](#)
- features [345](#)
- ping [345](#)
- status [346](#)

Differentiated Services [158](#)

Diffie-Hellman key group [223](#)

- Perfect Forward Secrecy (PFS) [229](#)

DiffServ [158](#)

DiffServ Code Point (DSCP) [158](#)

DiffServ Code Points [158](#)

DiffServ, marking rule [159](#)

directory servers

- adding/editing [271](#)
- certificates [250](#)

directory servers, and certificates [270](#)

disclaimer [3](#)

DMZ

- and remote management [293](#)

DNS [302](#)

- and remote management [302](#)

DNS (Domain Name System) [106](#), [302](#)

DNS, dynamic [289](#)

documentation [39](#)

domain name [107](#)

Domain Name System (DNS) [106](#), [302](#)

Domain Name System, See DNS

domain name, and ISPs [319](#)

domain name, of system [319](#)

DoS [189](#)

types [190](#)

DoS (Denial of Service)

basics [189](#)

DoS thresholds, and firewall [213](#)

DoS, attacks [190](#)

DS Field [158](#)

DS field [158](#)

DSCPs [158](#)

DSL line

diagnostics [345](#)

DTMF [156](#)

DTMF Detection and Generation [366](#)

Dual-Tone Multi-Frequency [156](#)

dynamic DNS [289](#), [290](#)

and DHCP [289](#)

and ISPs [289](#)

and services [289](#)

and WAN [289](#)

configuration [290](#)

wildcard feature [289](#)

Dynamic Jitter Butter [366](#)

## E

EAP-MD5 [365](#)

Echo Cancellation [366](#)

echo cancellation [167](#)

e-mail

and logs [327](#)

E-Mail, application priority [137](#)

emergency numbers, and VoIP [185](#)

Encapsulated Routing Link Protocol (ENET ENCAP) [89](#)

Encapsulating Security Payload. See ESP.

encapsulation [89](#)

and active protocol [228](#)

ENET ENCAP [89](#)

multiprotocol [90](#)

PPP over Ethernet [89](#)

PPPoA [90](#)

RFC 1483 [90](#)

transport mode [229](#)

tunnel mode [228](#)

VPN [228](#)

encryption algorithms [223](#)

and active protocol [223](#)

encryption, wireless [128](#)

errors, types of logs [325](#)

ESP [228](#)

and transport mode [229](#)

Ethernet lights [349](#)

Europe type call service mode [168](#)

Europe type supplementary services [168](#)

extended authentication

IKE SA [225](#)

Extended Service Set IDentification [124](#)

extended wireless security [63](#)

External RADIUS [365](#)

## F

F4/F5 OAM [364](#)

factory defaults [336](#)

fairness-based bandwidth management [279](#)

FCC interference statement [4](#)

file names, and configuration [331](#)

filename conventions [332](#)

filtering content [217](#)

filters vs. firewalls [197](#)

firewall [209](#)

access methods [199](#)

address type [207](#)

alert [215](#)

alerts [202](#)

and file maintenance [332](#)

and ICMP [303](#)

and remote management [293](#)

anti-probing [213](#)

creating/editing rules [205](#)

custom ports [208](#)

default policy [199](#)

DoS threshold [213](#)

enabling [202](#)

example [209](#)

example rule [209](#)

LAN to WAN rules [202](#)

policies [199](#)

rule checklist [200](#)

rule example [200](#)

rule logic [200](#)

rule security ramifications [200](#)

rules [200](#)

key fields [201](#)

types [187](#)

web configurator [199](#)

firewalls [195](#)

and brute-force attacks [191](#)

and handshake [190](#)

and IP Spoofing [193](#)

and LAND [190](#)

and Ping of Death [190](#)

- and Smurf attack [191](#)
- and SYN attack [191](#)
- and SYN Flood [190](#)
- and TCP/IP [190](#)
- and Teardrop [190](#)
- and three-way-handshake [190](#)
- and upper layer protocols [196](#)
- application level [188](#)
- denial of service [188](#)
- guidelines for enhancing security [196](#)
- introduction, ZyXEL [188](#)
- packet filtering [187](#)
- upper layer protocols [195](#)
- when to use [198](#)

firewalls vs. filters [197](#)

firmware [331](#)

- and FTP [332](#)
- and HTTP [332](#)
- upload [332](#), [341](#)
- upload error [334](#)
- upload example [331](#)
- uploading [331](#)
- version [332](#)

firmware.bin [331](#)

flash key, VoIP [168](#)

frequency pairs [156](#)

Frequency Range [365](#)

FTP [144](#), [293](#), [298](#)

- and remote management [298](#)
- firmware [332](#)
- firmware upgrade [298](#)
- firmware upload example [331](#)
- restoring configuration [340](#)

## G

G.168 [167](#), [366](#)

G.711 [156](#), [366](#)

G.729 [156](#), [366](#)

G.992.1 [364](#)

G.992.3 [364](#)

G.992.4 [364](#)

G.992.5 [364](#)

general setup [319](#)

- configuration [320](#)

graphics icons [40](#)

group ring [181](#)

## H

half-open sessions, and firewall [214](#)

hardware

- problems [349](#)

HTTP [188](#), [189](#), [190](#)

- and firmware [332](#)
- and remote management [293](#)

HTTPS [294](#)

- and remote management [293](#), [294](#)
- implementation [295](#)
- introduction [294](#)

Humidity [361](#)

hybrid, waveform codec [156](#)

## I

IAD (Integrated Access Device) [41](#)

IANA [108](#)

IANA, IP address assignment [108](#)

ICMP

- and anti-probing [303](#)
- and firewall [303](#)
- and LAN [303](#)
- and remote management [302](#)
- and WAN [303](#)
- response packets [303](#)

ICMP (Internet Control Message Protocol) [303](#)

ICMP echo [191](#)

icons, graphics [40](#)

IEEE 802.1Q VLAN [159](#)

IGMP [109](#)

IGMP Proxy [364](#)

IGMP v1 [364](#)

IGMP v2 [364](#)

IGMP, versions [109](#)

IKE SA

- aggressive mode [222](#), [226](#)
- and certificates [225](#)
- and RADIUS [225](#)
- authentication algorithms [223](#)
- Diffie-Hellman key group [223](#)
- encryption algorithms [223](#)
- extended authentication [225](#)
- ID content [224](#)
- ID type [224](#)
- IP address, remote IPSec router [222](#)
- IP address, ZyXEL Device [222](#)
- local identity [224](#)
- main mode [222](#), [226](#)
- NAT traversal [227](#)
- negotiation mode [222](#)



- password [225](#)
  - peer identity [224](#)
  - pre-shared key [224](#)
  - proposal [223](#)
  - user name [225](#)
  - IKE SA. See also VPN.
  - importing certificates [253](#)
  - importing trusted CA's [261](#)
  - importing trusted remote hosts [267](#)
  - installing
    - UPnP [309](#)
  - Integrated Access Device (IAD) [41](#)
  - Internal SPTGEN [415](#)
    - FTP Upload Example [417](#)
    - Points to Remember [415](#)
    - Text File [415](#)
  - Internet access [42, 53](#)
    - backup [102](#)
    - setup [350](#)
  - Internet access wizard setup [53](#)
  - Internet Assigned Numbers Authority see IANA [108](#)
  - Internet Control Message Protocol (ICMP) [191, 303](#)
  - Internet Control Message Protocol, See ICMP [303](#)
  - Internet Protocol Security. See IPSec.
  - Internet settings [351](#)
  - Internet Telephony Service Provider (ITSP) [151](#)
  - IP address [107, 144](#)
  - IP address assignment [91, 107](#)
    - ENET ENCAP [91](#)
    - IANA rules [108](#)
    - PPPoA or PPPoE [91](#)
    - RFC 1483 [91](#)
  - IP address range [113](#)
  - IP Multicasting [364](#)
  - IP pool [113](#)
  - IP pool setup [106](#)
  - IP spoofing [190](#)
  - IP Spoofing, and firewalls [193](#)
  - IP-PBX [151](#)
  - IPSec [221](#)
  - IPSec Passthrough [365](#)
  - IPSec SA
    - active protocol [228](#)
    - authentication algorithms [223](#)
    - authentication key (manual keys) [230](#)
    - encapsulation [228](#)
    - encryption algorithms [223](#)
    - encryption key (manual keys) [230](#)
    - local policy [228](#)
    - manual keys [229](#)
    - Perfect Forward Secrecy (PFS) [229](#)
    - proposal [229](#)
    - remote policy [228](#)
    - Security Parameter Index (SPI) (manual keys) [230](#)
    - transport mode [229](#)
    - tunnel mode [228](#)
    - when IKE SA is disconnected [227](#)
  - IPSec SA. See also VPN.
  - IPSec. See also VPN.
  - ISP
    - and domain name [319](#)
  - ISP issues [350](#)
  - ITSP [151](#)
  - ITU-T [167](#)
- ## J
- Java permissions [351](#)
  - JavaScript permissions [351](#)
- ## K
- key fields for configuring rules [201](#)
  - keys and certificates [249](#)
  - keyword blocking [217](#)
- ## L
- LAN
    - and bandwidth management [277](#)
    - and ICMP [303](#)
    - and remote management [293](#)
    - firewall policy [199](#)
    - problems [349](#)
  - LAN setup [105](#)
  - LAN TCP/IP [107](#)
  - LAN to WAN rules [202](#)
  - LAND, and firewalls [190](#)
  - listening port [164](#)
  - LLC [90](#)
  - log out [47](#)
  - logs [325](#)
    - activating [327](#)
    - alerts [325, 326](#)
    - and email [327](#)
    - and web configurator [325](#)
    - configuration [326, 327](#)
    - DSL line [347](#)
    - errors [325](#)
    - example [329](#)
    - navigating in [325](#)

- schedule [327](#)
- settings [326](#)
- sorting [325](#)
- syslog server [325](#)
- viewing [325](#)

## M

- MAC address filter action [134](#)
- MAC filter [134](#)
- Management Information Base (MIB) [299](#)
- Management Information Base, See MIB
- management software, SNMP [299](#)
- management tools [331](#)
- mapping rules, and NAT [148](#)
- maximizing bandwidth usage [279](#)
- Maximum Burst Size (MBS) [93](#), [98](#)
- max-incomplete high, and firewall [214](#)
- metric [92](#)
- metric, as a cost of transmission [92](#)
- MIB
  - and SNMP [299](#)
  - supported by ZyXEL Device [300](#)
- MIB (Management Information Base) [299](#)
- monitoring, and bandwidth management [287](#)
- multicasting [109](#)
- multimedia sessions, and SIP [151](#)
- multiplexing [90](#)
  - LLC-based [90](#)
  - VC-based [90](#)
- multiprotocol encapsulation [90](#)

## N

- nailed-up connection [91](#)
- name conventions [331](#)
- name conventions, table [332](#)
- NAT [107](#), [144](#)
  - address mapping rule [148](#)
  - and remote management [294](#)
  - and SIP [155](#)
  - and STUN [155](#)
  - and UPnP [307](#)
  - and VPN [226](#)
  - application [141](#)
  - definitions [139](#)
  - how it works [140](#)
  - mapping types [141](#)
  - modes [143](#)

- port forwarding [144](#)
- rules [148](#)
- server mapping [141](#)
- services [144](#)
- traversal [307](#)
  - what it does [140](#)
- NAT (Network Address Translation) [139](#)
- NAT routers [155](#)
- NAT Sessions [365](#)
- NAT traversal [227](#)
- NAT vs. SUA [142](#)
- NetBIOS commands [192](#)

## O

- OAM [364](#)
- Operation Humidity [361](#)
- Operation Temperature [361](#)
- outbound proxy server [156](#)
- outbound proxy, and SIP [155](#)
- outbound proxy, SIP [156](#)
- outbound proxy, VoIP [156](#)

## P

- packet filtering [197](#)
  - when to use [198](#)
- packet filtering firewalls [187](#)
- password
  - and web configurator [320](#)
  - changing [46](#), [320](#)
- PBX services [151](#)
- PCM [156](#)
- Peak Cell Rate (PCR) [92](#), [98](#)
- peer-to-peer calls [41](#), [177](#)
- Perfect Forward Secrecy (PFS)
  - Diffie-Hellman key group [229](#)
- Per-Hop Behavior [158](#)
- Permanent Virtual Circuits [364](#)
- PHB (Per-Hop Behavior) [159](#)
- phone book [177](#)
- phone ports [359](#)
- Ping of Death, and firewalls [190](#)
- PKI (Public-Key Infrastructure) [250](#)
- Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [90](#)
- Point-to-point Calls [366](#)
- POP3 [189](#), [190](#)

pop-ups, browser settings [351](#)  
 Port Forwarding [365](#)  
 port forwarding [144](#)  
   and servers [144](#)  
   configuration [145](#)  
   example [144](#)  
 Power Adaptor [366](#)  
 Power Adaptor Specifications [366](#)  
 PPP (Point-to-Point Protocol) Link Layer Protocol [364](#)  
 PPP over ATM AAL5 [364](#)  
 PPP over Ethernet [364](#)  
 PPPoE [89](#)  
   benefits [89](#)  
 PPPoE (Point-to-Point Protocol over Ethernet) [89](#)  
 priority based bandwidth management [278](#)  
 private keys, and remote management [294](#)  
 problems  
   hardware [349](#)  
   LAN [349](#)  
   lights [349](#)  
   powering up [349](#)  
   WAN [350](#)  
 problems, and diagnostics [345](#)  
 product registration [8](#)  
 proxy server, SIP [153](#)  
 PSTN [156](#)  
 PSTN line [185](#), [186](#)  
   configuration [186](#)  
   emergency numbers [185](#)  
   prefix number [186](#)  
   using [186](#)  
 public keys, and remote management [294](#)  
 Public Switched Telephone Network [156](#)  
 public-key cryptology, and certificates [249](#)  
 public-private keys  
   and certificates [249](#)  
 Pulse Code Modulation [156](#)  
 pulse dialing [156](#)  
 PVCs [364](#)

## Q

QoS, and VoIP [158](#)  
 QoS, wireless [135](#)  
 Quality of Service [158](#)  
 Quick Dialing [366](#)  
 quick start guide [39](#), [45](#)

## R

RADIUS [365](#)  
   and IKE SA [225](#)  
 Reach-Extended ADSL [364](#)  
 Real Time E-mail Alerts [365](#)  
 Real Time Transport Protocol [154](#)  
 recommended browser settings [351](#)  
 redirect server, SIP [154](#)  
 register server, SIP [154](#)  
 registration  
   product [8](#)  
 reinitialize the ADSL line [347](#)  
 related documentation [39](#)  
 remote hosts, and certificates [264](#)  
 remote management [293](#)  
   and certificates [294](#)  
   and firewall [293](#)  
   and HTTPS [294](#)  
   and interfaces [293](#)  
   and NAT [294](#)  
   and private/public keys [294](#)  
   and SNMP [299](#), [300](#)  
   and SSL [294](#)  
   configuring DNS [302](#)  
   configuring FTP [298](#)  
   configuring ICMP [302](#)  
   configuring Telnet [296](#)  
   configuring WWW [295](#)  
   HTTPS example [295](#)  
   idle timeout [294](#)  
   limitations [293](#)  
   priority [293](#)  
   sessions [293](#)  
   troubleshooting [351](#)  
 Reports and Logs [365](#)  
 required bandwidth, and VoIP [156](#)  
 reset button [48](#)  
 resetting your device [48](#)  
 restart [331](#)  
 restore configuration  
   configuration file  
   restore [335](#)  
 restoring configuration  
   FTP [340](#)  
 restoring factory defaults [336](#)  
 RFC 1483 [90](#), [364](#)  
 RFC 1631 [139](#)  
 RFC 1889 [154](#), [366](#)  
 RFC 1890 [366](#)  
 RFC 2327 [366](#)  
 RFC 2364 [364](#)  
 RFC 2516 [364](#)

RFC 2684 [364](#)  
RFC 3261 [366](#)  
RFC 3489 [155](#)  
RIP [108](#)  
    direction [108](#)  
    version [108](#)  
RIP (Routing Information Protocol) [108](#)  
romfile, configuration file [331](#)  
root class, and bandwidth management [280](#)  
router features [42](#)  
routing, static route [273](#)  
RTCP [366](#)  
RTP [154](#), [366](#)  
rules  
    LAN to WAN [202](#)  
rules, and bandwidth management [283](#)  
rules, and firewall [200](#)

## S

safety warnings [6](#)  
saving the state, and stateful inspection [193](#)  
scheduler, and bandwidth management [278](#)  
scheduling bandwidth management [278](#)  
scheduling logs [327](#)  
SDP [366](#)  
Seamless Rate Adaptation [364](#)  
Secure Socket Layer (SSL) [294](#)  
security  
    and certificates [249](#)  
    browser settings [351](#)  
    firewall example [209](#)  
    in general [196](#)  
    packet filtering [197](#)  
    remote management [302](#)  
security guidelines, and firewalls [196](#)  
security ramifications, and firewall [200](#)  
server mapping, NAT [141](#)  
server, outbound proxy [156](#)  
Service Type [350](#)  
service type, and firewalls [209](#)  
services, and NAT [144](#)  
Session Description Protocol [366](#)  
Session Initiating Protocol [366](#)  
Session Initiation Protocol (SIP) [151](#)  
Silence Suppression [366](#)  
silence suppression [167](#)  
silent packets [167](#)  
Simple Network Management Protocol (SNMP) [299](#)  
Simple Network Management Protocol, See SNMP  
SIP [151](#)  
SIP account [151](#)  
SIP accounts [67](#)  
SIP ALG [149](#), [155](#)  
SIP ALG Passthrough [365](#)  
SIP Application Layer Gateway [149](#)  
SIP call progression [152](#)  
SIP client [152](#)  
SIP client server [152](#)  
SIP identities [151](#)  
SIP INVITE request [152](#)  
SIP number [69](#), [151](#)  
SIP outbound proxy [156](#)  
SIP proxy server [153](#)  
SIP redirect server [154](#)  
SIP register server [154](#)  
SIP server address [69](#)  
SIP servers [152](#)  
SIP Service Domain [152](#)  
SIP service domain [70](#)  
SIP URI [151](#)  
SIP user agent [153](#)  
SIP Version 2 [366](#)  
SIP, authentication password [70](#)  
SIP, authentication user ID [70](#)  
SMTP  
    error messages [329](#)  
SMTP Error Messages [329](#)  
Smurf attack example [192](#)  
SNMP [299](#), [364](#)  
    agent [299](#)  
    and MIB [299](#)  
    and remote management [299](#), [300](#)  
    and TCP/IP [299](#)  
    management model [299](#)  
    manager [299](#)  
    MIBs [300](#)  
    traps [300](#)  
SNMP (Simple Network Management Protocol) [299](#)  
sound quality, and VoIP [156](#)  
source address, and firewall [201](#)  
speed dial [177](#)  
SRA [364](#)  
SSL (Secure Socket Layer) [294](#)  
stateful inspection [187](#), [188](#), [193](#)  
    on your ZyXEL Device [194](#)  
    process [194](#)  
stateful inspection example [193](#)  
Stateful Packet Inspection [365](#)  
static route [273](#)  
    and remote nodes [273](#)

- configuration [274](#)
- example [273](#)
- reaching other networks [273](#)
- Storage Humidity [361](#)
- Storage Temperature [361](#)
- STUN [155](#)
  - how it works [155](#)
- SUA [142](#)
- SUA (Single User Account) [142](#)
- SUA vs. NAT [142](#)
- subnet [379](#)
- subnet based bandwidth management [278](#)
- subnet mask [107](#), [381](#)
- subnetting [381](#)
- supplementary phone services [167](#)
- supplementary services, VoIP [167](#)
- supporting disk [39](#)
- Sustain Cell Rate (SCR) [98](#)
- Sustained Cell Rate (SCR) [92](#)
- SYN attack, and firewalls [191](#)
- SYN Flood, and firewalls [190](#)
- syntax conventions [39](#)
- syslog server, and logs [325](#)
- system name [319](#)
- System Parameter Table Generator [415](#)
- system time [321](#)
- system timeout [294](#)

## T

- TCP security [195](#)
- TCP/IP
  - and SNMP [299](#)
- TCP/IP, and firewalls [189](#), [190](#)
- Teardrop, and firewalls [190](#)
- telephone keys [156](#)
- telephone problems [359](#)
- Telnet [296](#)
  - and remote management [296](#)
  - example of remote management [297](#)
- Temperature [361](#)
- Text File Format [415](#)
- three-way conference [169](#), [170](#)
- three-way handshake, and firewalls [190](#)
- threshold values, and firewall [213](#)
- time [321](#)
  - daylight saving [321](#)
  - server [321](#)
  - settings [321](#)

- zone [321](#)
- time server [321](#)
- TLS [365](#)
- tools, for management [331](#)
- ToS [158](#)
- Touch Tone® [156](#)
- traceroute, and firewalls [193](#)
- trademarks [3](#)
- traffic priority
  - wireless [135](#)
- traffic redirect [102](#), [103](#), [104](#)
- traffic redirect example [102](#)
- traffic shaping [92](#)
- transferring a call [169](#), [170](#)
- Transparent Bridging [364](#)
- Triangle [399](#)
- Triangle Route Solutions [400](#)
- troubleshooting [349](#)
- trusted CAs, and certificates [259](#)
- trusted computers, and content filtering [219](#)
- TTLS [365](#)
- Type Of Service [158](#)

## U

- UBR (Unspecified Bit Rate) [98](#)
- UDP/ICMP security [195](#)
- Uniform Resource Identifier (URI) [151](#)
- Universal Plug and Play (UPnP) [307](#)
- Universal Plug and Play, See UPnP [307](#)
- UPnP [307](#)
  - and NAT [307](#)
  - and web configurator [315](#)
  - application [307](#)
  - configuration [308](#)
  - example [312](#)
  - Forum [308](#)
  - installation examples [309](#)
  - security issues [308](#)
  - Windows OS [309](#), [311](#)
- UPnP (Universal Plug and Play) [307](#)
- upper layer protocols, and firewalls [195](#), [196](#)
- USA type call service mode [170](#)
- user agent, SIP [153](#)

## V

- VAD [167](#), [366](#)

- VBR-nRT [98](#)
- VBR-RT [98](#)
- VCI (Virtual Channel Identifier) [90](#)
- Virtual Channel Identifier (VCI) [90](#)
- virtual circuit (VC), and multiplexing [90](#)
- Virtual Local Area Network [159](#)
- Virtual Path Identifier (VPI) [90](#)
- virtual private networks. See VPN.
- VLAN [159](#)
- VLAN group [159](#)
- VLAN ID [159](#)
- VLAN ID tags [159](#)
- VLAN tag [159](#)
- Voice Activity Detection [366](#)
- Voice Activity Detection (VAD) [167](#)
- voice coding [156](#)
- voice mail [151](#)
- Voice over IP (VoIP) [151](#)
- Voice over IP, see also VoIP [151](#)
- VoIP
  - account details [69](#)
  - call forwarding [179](#)
  - call policy [179](#)
  - conference calls [169](#), [170](#)
  - emergency numbers [185](#)
  - Europe [168](#)
  - outbound proxy [156](#)
  - phone book [177](#)
  - required bandwidth [156](#)
  - ring selection [181](#)
  - supplementary services [167](#)
  - testing rings [182](#)
  - transferring a call [170](#)
  - troubleshooting [359](#)
  - wizard example [69](#)
- VoIP features [41](#)
- VoIP setup, wizard [67](#)
- VPI & VCI [90](#)
- VPI (Virtual Path Identifier) [90](#)
- VPN [221](#)
  - active protocol [228](#)
  - and NAT [226](#)
  - established in two phases [221](#)
  - IKE SA. See IKE SA.
  - IPSec [221](#)
  - IPSec SA. See IPSec SA.
  - local network [221](#)
  - proposal [223](#)
  - remote IPSec router [221](#)
  - remote network [221](#)
  - security association (SA) [221](#)
- VPN. See also IKE SA, IPSec SA. [221](#)

## W

- WAN
  - and bandwidth management [277](#)
  - and configuration file [332](#)
  - and dynamic DNS [289](#)
  - and ICMP [303](#)
  - and remote management [293](#)
  - file maintenance [332](#)
  - firewall policy [199](#)
  - problems [350](#)
- WAN (Wide Area Network) [89](#)
- WAN setup [89](#)
- WAN to LAN rules [202](#)
- warranty [8](#)
  - note [8](#)
- waveform codec [156](#)
- web configurator [45](#)
  - and logs [325](#)
  - and password [320](#)
  - and UPnP [315](#)
  - automatic log out [47](#)
  - default IP [45](#)
  - firewall [196](#), [199](#), [201](#)
  - login [45](#)
  - password [45](#)
  - problems accessing [349](#)
  - restart [331](#)
- web, and remote management [295](#)
- WEP encryption [127](#)
- wireless
  - channel ID [124](#)
  - MAC filter [134](#)
  - priority [135](#)
  - QoS [135](#)
  - security
    - WEP [127](#)
    - WPA [128](#)
    - WPA-PSK [126](#)
    - security mode [123](#)
- wireless LAN setup [123](#)
- wireless setup, wizard [60](#)
- wizards
  - bandwidth management [73](#)
  - Internet access [53](#)
  - VoIP [67](#)
  - wireless setup [60](#)
- WLAN
  - and bandwidth management [277](#)
- WPA [128](#)
- WPA-PSK [126](#)
- WWW
  - and remote management [295](#)
- WWW, application priority [137](#)

## Z

zero configuration Internet access [94](#)

ZyNOS [332](#)

ZyNOS (ZyXEL Network Operating System) [331](#)

ZyNOS firmware version [332](#)

ZyXEL's firewall  
introduction [188](#)