

P-662H/HW-D Series

802.11g ADSL 2+ 4-Port Security Gateway

User's Guide

Version 3.40
Edition 1
7/2006

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is in a smaller font size than "XEL", and the "X" is significantly larger and more prominent.

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

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

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation

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

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

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.

FCC Caution

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

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

ZyXEL Communications Corporation declared that P-662H/HW-D is limited in CH1~11 from 2400 to 2483.5 MHz by specified firmware controlled in USA.

Viewing Certifications

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

Safety Warnings

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

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

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.

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

Copyright	3
Certifications	4
Safety Warnings	6
ZyXEL Limited Warranty	7
Customer Support	8
Table of Contents	11
List of Figures	25
List of Tables	33
Preface	39
Chapter 1	
Getting To Know Your ZyXEL Device	41
1.1 Introducing the ZyXEL Device	41
1.1.1 Features of the ZyXEL Device	41
1.1.1.1 P-662HW Wireless Features	45
1.1.2 Applications for the ZyXEL Device	45
1.1.2.1 Internet Access	46
1.1.2.2 LAN to LAN Application	46
1.1.3 Firewall for Secure Broadband Internet Access	46
1.1.4 Front Panel LEDs	47
Chapter 2	
Introducing the Web Configurator	49
2.1 Web Configurator Overview	49
2.2 Accessing the Web Configurator	49
2.3 Resetting the ZyXEL Device	51
2.3.1 Using the Reset Button	52
2.4 Navigating the Web Configurator	52
2.4.1 Navigation Panel	52
2.4.2 Status Screen	55
2.4.3 Status: Any IP Table.....	58
2.4.4 Status: WLAN Status	58
2.4.5 Status: Bandwidth Status	59

2.4.6 Status: VPN Status	59
2.4.7 Status: Packet Statistics.....	60
2.4.8 Changing Login Password	62
Chapter 3	
Wizard Setup for Internet Access	65
3.1 Introduction	65
3.2 Internet Access Wizard Setup	65
3.2.1 Automatic Detection	67
3.2.2 Manual Configuration	67
3.3 Wireless Connection Wizard Setup	72
3.3.1 Automatically assign a WPA key	75
3.3.2 Manually assign a WPA-PSK key	75
3.3.3 Manually assign a WEP key	76
Chapter 4	
Bandwidth Management Wizard	79
4.1 Introduction	79
4.2 Predefined Media Bandwidth Management Services	79
4.3 Bandwidth Management Wizard Setup	80
Chapter 5	
WAN Setup.....	85
5.1 WAN Overview	85
5.1.1 Encapsulation	85
5.1.1.1 ENET ENCAP	85
5.1.1.2 PPP over Ethernet	85
5.1.1.3 PPPoA	86
5.1.1.4 RFC 1483	86
5.1.2 Multiplexing	86
5.1.2.1 VC-based Multiplexing	86
5.1.2.2 LLC-based Multiplexing	86
5.1.3 VPI and VCI	86
5.1.4 IP Address Assignment	87
5.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation	87
5.1.4.2 IP Assignment with RFC 1483 Encapsulation	87
5.1.4.3 IP Assignment with ENET ENCAP Encapsulation	87
5.1.5 Nailed-Up Connection (PPP)	87
5.1.6 NAT	87
5.2 Metric	88
5.3 Traffic Shaping	88
5.3.1 ATM Traffic Classes	89
5.3.1.1 Constant Bit Rate (CBR)	89

5.3.1.2 Variable Bit Rate (VBR)	89
5.3.1.3 Unspecified Bit Rate (UBR)	90
5.4 Zero Configuration Internet Access	90
5.5 Internet Connection	90
5.5.1 Configuring Advanced Internet Connection	92
5.6 Configuring More Connections	94
5.6.1 More Connections Edit	95
5.6.2 Configuring More Connections Advanced Setup	98
5.7 Traffic Redirect	99
5.8 Configuring WAN Backup	100
5.9 WAN Backup Advanced Screen	102
5.10 Dial Backup Modem Setup	105
Chapter 6	
LAN Setup	109
6.1 LAN Overview	109
6.1.1 LANs, WANs and the ZyXEL Device	109
6.1.2 DHCP Setup	110
6.1.2.1 IP Pool Setup	110
6.1.3 DNS Server Address	110
6.1.4 DNS Server Address Assignment	111
6.2 LAN TCP/IP	111
6.2.1 IP Address and Subnet Mask	111
6.2.1.1 Private IP Addresses	112
6.2.2 RIP Setup	112
6.2.3 Multicast	113
6.2.4 Any IP	113
6.2.4.1 How Any IP Works	114
6.3 Configuring LAN IP	115
6.3.1 Configuring Advanced LAN Setup	115
6.4 DHCP Setup	117
6.5 LAN Client List	118
6.6 LAN IP Alias	119
Chapter 7	
Wireless LAN	123
7.1 Wireless Network Overview	123
7.2 Wireless Security Overview	124
7.2.1 SSID	124
7.2.2 MAC Address Filter	124
7.2.3 User Authentication	124
7.2.4 Encryption	125
7.2.5 One-Touch Intelligent Security Technology (OTIST)	126

7.3 Wireless Performance Overview	126
7.3.1 Quality of Service (QoS)	126
7.4 Additional Wireless Terms	127
7.5 General Wireless LAN Screen	127
7.5.1 No Security	129
7.5.2 WEP Encryption Screen	129
7.5.3 WPA(2)-PSK	130
7.5.4 WPA(2) Authentication Screen	132
7.5.5 Wireless LAN Advanced Setup.....	134
7.6 OTIST	135
7.6.1 Enabling OTIST	135
7.6.1.1 AP	136
7.6.1.2 Wireless Client	137
7.6.2 Starting OTIST	138
7.6.3 Notes on OTIST	138
7.7 MAC Filter	139
7.8 WMM QoS	141
7.8.1 WMM QoS Example	141
7.8.2 WMM QoS Priorities	141
7.8.3 Services	142
7.9 QoS Screen	144
7.9.1 ToS (Type of Service) and WMM QoS	144
7.9.2 Application Priority Configuration.....	146
7.10 Multiple SSID (P-662HW-D Models only)	147
7.10.1 Multiple SSID Commands	148
7.10.2 Multiple SSID Example	150
Chapter 8	
DMZ	151
8.1 Introduction	151
8.2 Configuring DMZ	151
8.3 DMZ Public IP Address Example	153
8.4 DMZ Private and Public IP Address Example	154
Chapter 9	
Network Address Translation (NAT) Screens	157
9.1 NAT Overview	157
9.1.1 NAT Definitions	157
9.1.2 What NAT Does	158
9.1.3 How NAT Works	158
9.1.4 NAT Application	159
9.1.5 NAT Mapping Types	159
9.2 SUA (Single User Account) Versus NAT	160

9.3 NAT General Setup	160
9.4 Port Forwarding	161
9.4.1 Default Server IP Address	162
9.4.2 Port Forwarding: Services and Port Numbers	162
9.4.3 Configuring Servers Behind Port Forwarding (Example)	163
9.5 Configuring Port Forwarding	163
9.5.1 Port Forwarding Rule Edit	164
9.6 Address Mapping	165
9.6.1 Address Mapping Rule Edit	167

Chapter 10

Firewalls 169

10.1 Firewall Overview	169
10.2 Types of Firewalls	169
10.2.1 Packet Filtering Firewalls	169
10.2.2 Application-level Firewalls	170
10.2.3 Stateful Inspection Firewalls	170
10.3 Introduction to ZyXEL's Firewall	170
10.3.1 Denial of Service Attacks	171
10.4 Denial of Service	171
10.4.1 Basics	171
10.4.2 Types of DoS Attacks	172
10.4.2.1 ICMP Vulnerability	174
10.4.2.2 Illegal Commands (NetBIOS and SMTP)	174
10.4.2.3 Traceroute	175
10.5 Stateful Inspection	175
10.5.1 Stateful Inspection Process	176
10.5.2 Stateful Inspection and the ZyXEL Device	176
10.5.3 TCP Security	177
10.5.4 UDP/ICMP Security	177
10.5.5 Upper Layer Protocols	178
10.6 Guidelines for Enhancing Security with Your Firewall	178
10.6.1 Security In General	179
10.7 Packet Filtering Vs Firewall	179
10.7.1 Packet Filtering:	180
10.7.1.1 When To Use Filtering	180
10.7.2 Firewall	180
10.7.2.1 When To Use The Firewall	180

Chapter 11

Firewall Configuration 181

11.1 Access Methods	181
11.2 Firewall Policies Overview	181

11.3 Rule Logic Overview	182
11.3.1 Rule Checklist	182
11.3.2 Security Ramifications	182
11.3.3 Key Fields For Configuring Rules	183
11.3.3.1 Action	183
11.3.3.2 Service	183
11.3.3.3 Source Address	183
11.3.3.4 Destination Address	183
11.4 Connection Direction	183
11.4.1 LAN to WAN Rules	184
11.4.2 Alerts	184
11.5 General Firewall Policy	184
11.6 Firewall Rules Summary	185
11.6.1 Configuring Firewall Rules	187
11.6.2 Customized Services	190
11.6.3 Configuring A Customized Service	191
11.7 Example Firewall Rule	191
11.8 Predefined Services	195
11.9 Anti-Probing	197
11.10 DoS Thresholds	198
11.10.1 Threshold Values	198
11.10.2 Half-Open Sessions	199
11.10.2.1 TCP Maximum Incomplete and Blocking Time	199
11.10.3 Configuring Firewall Thresholds	200
Chapter 12	
Anti-Virus Packet Scan	203
12.1 Overview	203
12.1.1 Types of Computer Viruses	203
12.2 Signature-Based Virus Scan	203
12.2.1 Computer Virus Infection and Prevention	204
12.3 Introduction to the ZyXEL Device Anti-virus Packet Scan	204
12.3.1 How the ZyXEL Device Virus Scan Works	205
12.3.2 Limitations of the ZyXEL Device Packet Scan	205
12.4 Anti-Virus Packet Scan Configuration	205
12.5 Registration and Online Update	207
12.5.1 Updating the Anti-Virus Packet Scan	209
Chapter 13	
Content Filtering	211
13.1 Content Filtering Overview	211
13.2 Configuring Keyword Blocking	211
13.3 Configuring the Schedule	212

13.4 Configuring Trusted Computers	213
Chapter 14	
Content Access Control	215
14.1 Content Access Control Overview	215
14.1.1 Content Access Control WLAN Application	215
14.1.2 Configuration Steps	215
14.2 Activating CAC and Creating User Groups	216
14.2.1 Configuring Time Schedule	217
14.2.2 Configuring Services	219
14.2.2.1 Available Services	220
14.2.3 Configuring Web Site Filters	222
14.2.4 Testing Web Site Access Privileges	227
14.3 User Account Setup	228
14.4 User Online Status	229
14.5 Content Access Control Logins	230
14.5.1 User Login	230
14.5.2 Administrator Login	231
Chapter 15	
Introduction to IPSec	233
15.1 VPN Overview	233
15.1.1 IPSec	233
15.1.2 Security Association	233
15.1.3 Other Terminology	233
15.1.3.1 Encryption	233
15.1.3.2 Data Confidentiality	234
15.1.3.3 Data Integrity	234
15.1.3.4 Data Origin Authentication	234
15.1.4 VPN Applications	234
15.2 IPSec Architecture	235
15.2.1 IPSec Algorithms	235
15.2.2 Key Management	235
15.3 Encapsulation	235
15.3.1 Transport Mode	236
15.3.2 Tunnel Mode	236
15.4 IPSec and NAT	236
Chapter 16	
VPN Screens	239
16.1 VPN/IPSec Overview	239
16.2 IPSec Algorithms	239
16.2.1 AH (Authentication Header) Protocol	239

16.2.2 ESP (Encapsulating Security Payload) Protocol	239
16.3 My IP Address	240
16.4 Secure Gateway Address	241
16.4.1 Dynamic Secure Gateway Address	241
16.5 VPN Setup Screen	241
16.6 Keep Alive	243
16.7 VPN, NAT, and NAT Traversal	244
16.8 Remote DNS Server	245
16.9 ID Type and Content	245
16.9.1 ID Type and Content Examples	246
16.10 Pre-Shared Key	247
16.11 Editing VPN Policies	247
16.12 IKE Phases	252
16.12.1 Negotiation Mode	253
16.12.2 Diffie-Hellman (DH) Key Groups	254
16.12.3 Perfect Forward Secrecy (PFS)	254
16.13 Configuring Advanced IKE Settings	254
16.14 Manual Key Setup	257
16.14.1 Security Parameter Index (SPI)	257
16.15 Configuring Manual Key	257
16.16 Viewing SA Monitor	260
16.17 Configuring Global Setting	261
16.18 Telecommuter VPN/IPSec Examples	262
16.18.1 Telecommuters Sharing One VPN Rule Example	262
16.18.2 Telecommuters Using Unique VPN Rules Example	263
16.19 VPN and Remote Management	264
Chapter 17	
Certificates.....	265
17.1 Certificates Overview	265
17.1.1 Advantages of Certificates	266
17.2 Self-signed Certificates	266
17.3 Configuration Summary	266
17.4 My Certificates	267
17.5 My Certificate Import	269
17.5.1 Certificate File Formats	269
17.6 My Certificate Create	270
17.7 My Certificate Details	272
17.8 Trusted CAs	275
17.9 Trusted CA Import	277
17.10 Trusted CA Details	278
17.11 Trusted Remote Hosts	280
17.12 Verifying a Trusted Remote Host's Certificate	282

17.12.1 Trusted Remote Host Certificate Fingerprints	282
17.13 Trusted Remote Hosts Import	283
17.14 Trusted Remote Host Certificate Details	283
17.15 Directory Servers	286
17.16 Directory Server Add or Edit	287
Chapter 18	
Static Route	289
18.1 Static Route	289
18.2 Configuring Static Route	289
18.2.1 Static Route Edit	290
Chapter 19	
Bandwidth Management	293
19.1 Bandwidth Management Overview	293
19.2 Application-based Bandwidth Management	293
19.3 Subnet-based Bandwidth Management	293
19.4 Application and Subnet-based Bandwidth Management	294
19.5 Scheduler	294
19.5.1 Priority-based Scheduler	294
19.5.2 Fairness-based Scheduler	295
19.6 Maximize Bandwidth Usage	295
19.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic	295
19.6.2 Maximize Bandwidth Usage Example	296
19.6.2.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth	296
19.6.2.2 Fairness-based Allotment of Unused and Unbudgeted	
Bandwidth	297
19.6.3 Bandwidth Management Priorities	297
19.7 Configuring Summary	297
19.8 Bandwidth Management Rule Setup	299
19.8.1 Rule Configuration	300
19.9 Bandwidth Monitor	302
Chapter 20	
Dynamic DNS Setup.....	305
20.1 Dynamic DNS Overview	305
20.1.1 DYNDNS Wildcard	305
20.2 Configuring Dynamic DNS	305
Chapter 21	
Remote Management Configuration	309
21.1 Remote Management Overview	309
21.1.1 Remote Management Limitations	309

21.1.2 Remote Management and NAT	310
21.1.3 System Timeout	310
21.2 WWW	310
21.3 Telnet	311
21.4 Configuring Telnet	311
21.5 Configuring FTP	312
21.6 SNMP	313
21.6.1 Supported MIBs	314
21.6.2 SNMP Traps	315
21.6.3 Configuring SNMP	315
21.7 Configuring DNS	317
21.8 Configuring ICMP	317
21.9 TR-069	319
Chapter 22	
Universal Plug-and-Play (UPnP)	321
22.1 Introducing Universal Plug and Play	321
22.1.1 How do I know if I'm using UPnP?	321
22.1.2 NAT Traversal	321
22.1.3 Cautions with UPnP	322
22.2 UPnP and ZyXEL	322
22.2.1 Configuring UPnP	322
22.3 Installing UPnP in Windows Example	323
22.4 Using UPnP in Windows XP Example	326
Chapter 23	
System	333
23.1 General Setup	333
23.1.1 General Setup and System Name	333
23.1.2 General Setup	333
23.2 Time Setting	335
Chapter 24	
Logs	339
24.1 Logs Overview	339
24.1.1 Alerts and Logs	339
24.2 Viewing the Logs	339
24.3 Configuring Log Settings	340
24.4 SMTP Error Messages	343
24.4.1 Example E-mail Log	343

Chapter 25	
Tools	345
25.1 Firmware Upgrade	345
25.2 Configuration Screen	347
25.2.1 Backup Configuration	347
25.2.2 Restore Configuration	348
25.2.3 Back to Factory Defaults	349
25.3 Restart	349
Chapter 26	
Diagnostic	351
26.1 General Diagnostic	351
26.2 DSL Line Diagnostic	352
Chapter 27	
Troubleshooting	353
27.1 Problems Starting Up the ZyXEL Device	353
27.2 Problems with the LAN	353
27.3 Problems with the WAN	354
27.4 Problems Accessing the ZyXEL Device	355
27.4.1 Pop-up Windows, JavaScripts and Java Permissions	355
27.4.1.1 Internet Explorer Pop-up Blockers	355
27.4.1.2 JavaScripts	358
27.4.1.3 Java Permissions	360
27.4.2 ActiveX Controls in Internet Explorer	362
Appendix A	
Product Specifications	365
Appendix B	
About ADSL	369
Introduction to DSL	369
ADSL Overview	369
Advantages of ADSL	369
Appendix C	
Wall-mounting Instructions	371
Appendix D	
Setting up Your Computer's IP Address	373
Windows 95/98/Me	373
Windows 2000/NT/XP	376
Macintosh OS 8/9	381

Macintosh OS X	383
Linux.....	384
Appendix E	
IP Addresses and Subnetting	389
Introduction to IP Addresses	389
Subnet Masks	391
Subnetting	391
Example: Two Subnets	392
Example: Four Subnets.....	393
Example Eight Subnets.....	394
Subnetting With Class A and Class B Networks	395
Appendix F	
Wireless LANs	397
Wireless LAN Topologies	397
Channel.....	399
RTS/CTS.....	399
Fragmentation Threshold	400
Preamble Type	401
IEEE 802.11g Wireless LAN	401
IEEE 802.1x	402
RADIUS.....	402
Types of Authentication.....	403
WPA(2).....	405
Security Parameters Summary	407
Appendix G	
Importing Certificates	409
Import ZyXEL Device Certificates into Netscape Navigator	409
Importing the ZyXEL Device's Certificate into Internet Explorer	409
Enrolling and Importing SSL Client Certificates	413
Using a Certificate When Accessing the ZyXEL Device Example	417
Appendix H	
Command Interpreter.....	419
Command Syntax.....	419
Access via Telnet	419
Command Usage	419
Appendix I	
Certificates Commands	421

Appendix J	
Boot Commands	425
Appendix K	
Firewall Commands	427
Appendix L	
NetBIOS Filter Commands	433
Introduction	433
Display NetBIOS Filter Settings	433
NetBIOS Filter Configuration.....	434
Appendix M	
Internal SPTGEN	437
Internal SPTGEN Overview	437
The Configuration Text File Format.....	437
Internal SPTGEN FTP Download Example.....	438
Internal SPTGEN FTP Upload Example	439
Command Examples.....	460
Appendix N	
Splitters and Microfilters	463
Connecting a POTS Splitter	463
Telephone Microfilters	463
ZyXEL Device With ISDN.....	464
Appendix O	
Log Descriptions.....	465
Log Commands.....	479
Log Command Example.....	480
Appendix P	
Triangle Route	481
The Ideal Setup.....	481
The “Triangle Route” Problem.....	481
The “Triangle Route” Solutions	482
IP Aliasing	482
Gateways on the WAN Side.....	483
Index.....	485

List of Figures

Figure 1 ZyXEL Device Internet Access Application	46
Figure 2 ZyXEL Device LAN-to-LAN Application Example	46
Figure 3 Firewall Application	47
Figure 4 P-662H Front Panel	47
Figure 5 P-662HW Front Panel	47
Figure 6 Password Screen	50
Figure 7 Change Password at Login	50
Figure 8 Replace Factory Default Certificate	51
Figure 9 Select a Mode	51
Figure 10 Web Configurator: Main Screen	52
Figure 11 Status Screen	56
Figure 12 Status: Any IP Table	58
Figure 13 Status: WLAN Status	59
Figure 14 Status: Bandwidth Status	59
Figure 15 Status: VPN Status	60
Figure 16 Status: Packet Statistics	61
Figure 17 System General	62
Figure 18 Select a Mode	65
Figure 19 Wizard: Welcome	66
Figure 20 Auto Detection: No DSL Connection	66
Figure 21 Auto Detection: Failed	67
Figure 22 Auto-Detection: PPPoE	67
Figure 23 Internet Access Wizard Setup: ISP Parameters	68
Figure 24 Internet Connection with PPPoE	69
Figure 25 Internet Connection with RFC 1483	69
Figure 26 Internet Connection with ENET ENCAP	70
Figure 27 Internet Connection with PPPoA	71
Figure 28 Connection Test Failed-1	72
Figure 29 Connection Test Failed-2.	72
Figure 30 Connection Test Successful	73
Figure 31 Wireless LAN Setup Wizard 1	73
Figure 32 Wireless LAN Setup Wizard 2	74
Figure 33 Manually assign a WPA key	76
Figure 34 Manually assign a WEP key	76
Figure 35 Wireless LAN Setup 3	77
Figure 36 Internet Access and WLAN Wizard Setup Complete	78
Figure 37 Select a Mode	80
Figure 38 Wizard: Welcome	81

Figure 39 Bandwidth Management Wizard: General Information	81
Figure 40 Bandwidth Management Wizard: Configuration	82
Figure 41 Bandwidth Management Wizard: Complete	83
Figure 42 Example of Traffic Shaping	89
Figure 43 Internet Connection (PPPoE)	91
Figure 44 Advanced Internet Connection	93
Figure 45 More Connections	95
Figure 46 More Connections Edit	96
Figure 47 More Connections Advanced Setup	98
Figure 48 Traffic Redirect Example	99
Figure 49 Traffic Redirect LAN Setup	100
Figure 50 WAN Backup Setup	101
Figure 51 WAN Backup Advanced Setup	103
Figure 52 WAN Dial Backup Modem Setup	106
Figure 53 LAN and WAN IP Addresses	109
Figure 54 Any IP Example	114
Figure 55 LAN IP	115
Figure 56 Advanced LAN Setup	116
Figure 57 DHCP Setup	117
Figure 58 LAN Client List	118
Figure 59 Physical Network & Partitioned Logical Networks	120
Figure 60 LAN IP Alias	120
Figure 61 Example of a Wireless Network	123
Figure 62 Wireless LAN: General	128
Figure 63 Wireless: No Security	129
Figure 64 Wireless: Static WEP Encryption	130
Figure 65 Wireless: WPA(2)-PSK	131
Figure 66 Wireless: WPA(2)	132
Figure 67 Advanced	134
Figure 68 OTIST	136
Figure 69 Example Wireless Client OTIST Screen	137
Figure 70 Security Key	138
Figure 71 OTIST in Progress (AP)	138
Figure 72 OTIST in Progress (Client)	138
Figure 73 No AP with OTIST Found	138
Figure 74 Start OTIST?	139
Figure 75 MAC Address Filter	140
Figure 76 Wireless LAN: QoS	145
Figure 77 Application Priority Configuration	146
Figure 78 Multiple SSID Network Example	148
Figure 79 DMZ	152
Figure 80 DMZ Public Address Example	154
Figure 81 DMZ Private and Public Address Example	155

Figure 82 How NAT Works	158
Figure 83 NAT Application With IP Alias	159
Figure 84 NAT General	161
Figure 85 Multiple Servers Behind NAT Example	163
Figure 86 NAT Port Forwarding	163
Figure 87 Port Forwarding Rule Setup	164
Figure 88 Address Mapping Rules	166
Figure 89 Edit Address Mapping Rule	167
Figure 90 Firewall Application	171
Figure 91 Three-Way Handshake	172
Figure 92 SYN Flood	173
Figure 93 Smurf Attack	174
Figure 94 Stateful Inspection	175
Figure 95 Firewall: General	184
Figure 96 Firewall Rules	186
Figure 97 Firewall: Edit Rule	188
Figure 98 Firewall: Customized Services	190
Figure 99 Firewall: Configure Customized Services	191
Figure 100 Firewall Example: Rules	192
Figure 101 Edit Custom Port Example	192
Figure 102 Firewall Example: Edit Rule: Destination Address	193
Figure 103 Firewall Example: Edit Rule: Select Customized Services	194
Figure 104 Firewall Example: Rules: MyService	195
Figure 105 Firewall: Anti Probing	197
Figure 106 Firewall: Threshold	200
Figure 107 ZyXEL Device Anti-virus Application	204
Figure 108 Anti-Virus: Packet Scan	206
Figure 109 Anti-Virus: Registration and Virus Information Update	208
Figure 110 Virus Scan Update in Progress	209
Figure 111 Virus Scan Update Successful	209
Figure 112 Content Filter: Keyword	211
Figure 113 Content Filter: Schedule	212
Figure 114 Content Filter: Trusted	213
Figure 115 Content Access Control with WLAN Application	215
Figure 116 Content Access Control: General	216
Figure 117 Control Access Control: General: Time Scheduling	218
Figure 118 Content Access Control: General: Services	219
Figure 119 Content Access Control: General: Web Site Filter	222
Figure 120 Content Access Control: General: Diagnose	227
Figure 121 Content Access Control: User Profiles	228
Figure 122 Content Access Control: Online Status	229
Figure 123 Content Access Control: User Login Screen	230
Figure 124 Content Access Control: User Logout Screen	230

Figure 125 Encryption and Decryption	234
Figure 126 IPSec Architecture	235
Figure 127 Transport and Tunnel Mode IPSec Encapsulation	236
Figure 128 IPSec Summary Fields	241
Figure 129 VPN Setup	242
Figure 130 NAT Router Between IPSec Routers	244
Figure 131 VPN Host using Intranet DNS Server Example	245
Figure 132 Edit VPN Policies	248
Figure 133 Two Phases to Set Up the IPSec SA	252
Figure 134 Advanced VPN Policies	255
Figure 135 VPN: Manual Key	258
Figure 136 VPN: SA Monitor	261
Figure 137 VPN: Global Setting	261
Figure 138 Telecommuters Sharing One VPN Rule Example	262
Figure 139 Telecommuters Using Unique VPN Rules Example	263
Figure 140 Certificate Configuration Overview	266
Figure 141 My Certificates	267
Figure 142 My Certificate Import	269
Figure 143 My Certificate Create	270
Figure 144 My Certificate Details	273
Figure 145 Trusted CAs	276
Figure 146 Trusted CA Import	277
Figure 147 Trusted CA Details	278
Figure 148 Trusted Remote Hosts	281
Figure 149 Remote Host Certificates	282
Figure 150 Certificate Details	282
Figure 151 Trusted Remote Host Import	283
Figure 152 Trusted Remote Host Details	284
Figure 153 Directory Servers	287
Figure 154 Directory Server Add	288
Figure 155 Example of Static Routing Topology	289
Figure 156 Static Route	290
Figure 157 Static Route Edit	291
Figure 158 Subnet-based Bandwidth Management Example	294
Figure 159 Bandwidth Management: Summary	298
Figure 160 Bandwidth Management: Rule Setup	299
Figure 161 Bandwidth Management Rule Configuration	300
Figure 162 Bandwidth Management: Monitor	303
Figure 163 Dynamic DNS	306
Figure 164 Remote Management: WWW	310
Figure 165 Telnet Configuration on a TCP/IP Network	311
Figure 166 Remote Management: Telnet	312
Figure 167 Remote Management: FTP	313

Figure 168 SNMP Management Model	314
Figure 169 Remote Management: SNMP	316
Figure 170 Remote Management: DNS	317
Figure 171 Remote Management: ICMP	318
Figure 172 Enabling TR-069	319
Figure 173 Configuring UPnP	322
Figure 174 Add/Remove Programs: Windows Setup: Communication	324
Figure 175 Add/Remove Programs: Windows Setup: Communication: Components	324
Figure 176 Network Connections	325
Figure 177 Windows Optional Networking Components Wizard	325
Figure 178 Networking Services	326
Figure 179 Network Connections	327
Figure 180 Internet Connection Properties	327
Figure 181 Internet Connection Properties: Advanced Settings	328
Figure 182 Internet Connection Properties: Advanced Settings: Add	328
Figure 183 System Tray Icon	329
Figure 184 Internet Connection Status	329
Figure 185 Network Connections	330
Figure 186 Network Connections: My Network Places	331
Figure 187 Network Connections: My Network Places: Properties: Example	331
Figure 188 System General Setup	334
Figure 189 System Time Setting	335
Figure 190 View Log	340
Figure 191 Log Settings	341
Figure 192 E-mail Log Example	343
Figure 193 Firmware Upgrade	345
Figure 194 Firmware Upload In Progress	346
Figure 195 Network Temporarily Disconnected	346
Figure 196 Error Message	347
Figure 197 Configuration	347
Figure 198 Configuration Restore Successful	348
Figure 199 Temporarily Disconnected	348
Figure 200 Configuration Restore Error	349
Figure 201 Restart Screen	349
Figure 202 Diagnostic: General	351
Figure 203 Diagnostic: DSL Line	352
Figure 204 Pop-up Blocker	356
Figure 205 Internet Options	356
Figure 206 Internet Options	357
Figure 207 Pop-up Blocker Settings	358
Figure 208 Internet Options	359
Figure 209 Security Settings - Java Scripting	360
Figure 210 Security Settings - Java	361

Figure 211 Java (Sun)	361
Figure 212 Internet Options Security	362
Figure 213 Security Setting ActiveX Controls	363
Figure 214 Wall-mounting Example	371
Figure 215 WInDows 95/98/Me: Network: Configuration	374
Figure 216 Windows 95/98/Me: TCP/IP Properties: IP Address	375
Figure 217 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	376
Figure 218 Windows XP: Start Menu	377
Figure 219 Windows XP: Control Panel	377
Figure 220 Windows XP: Control Panel: Network Connections: Properties	378
Figure 221 Windows XP: Local Area Connection Properties	378
Figure 222 Windows XP: Internet Protocol (TCP/IP) Properties	379
Figure 223 Windows XP: Advanced TCP/IP Properties	380
Figure 224 Windows XP: Internet Protocol (TCP/IP) Properties	381
Figure 225 Macintosh OS 8/9: Apple Menu	382
Figure 226 Macintosh OS 8/9: TCP/IP	382
Figure 227 Macintosh OS X: Apple Menu	383
Figure 228 Macintosh OS X: Network	384
Figure 229 Red Hat 9.0: KDE: Network Configuration: Devices	385
Figure 230 Red Hat 9.0: KDE: Ethernet Device: General	385
Figure 231 Red Hat 9.0: KDE: Network Configuration: DNS	386
Figure 232 Red Hat 9.0: KDE: Network Configuration: Activate	386
Figure 233 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	387
Figure 234 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	387
Figure 235 Red Hat 9.0: DNS Settings in resolv.conf	387
Figure 236 Red Hat 9.0: Restart Ethernet Card	388
Figure 237 Red Hat 9.0: Checking TCP/IP Properties	388
Figure 238 Peer-to-Peer Communication in an Ad-hoc Network	397
Figure 239 Basic Service Set	398
Figure 240 Infrastructure WLAN	399
Figure 241 RTS/CTS	400
Figure 242 Security Certificate	409
Figure 243 Login Screen	410
Figure 244 Certificate General Information before Import	410
Figure 245 Certificate Import Wizard 1	411
Figure 246 Certificate Import Wizard 2	411
Figure 247 Certificate Import Wizard 3	412
Figure 248 Root Certificate Store	412
Figure 249 Certificate General Information after Import	413
Figure 250 ZyXEL Device Trusted CA Screen	414
Figure 251 CA Certificate Example	414
Figure 252 Personal Certificate Import Wizard 1	415
Figure 253 Personal Certificate Import Wizard 2	415

Figure 254 Personal Certificate Import Wizard 3	416
Figure 255 Personal Certificate Import Wizard 4	416
Figure 256 Personal Certificate Import Wizard 5	417
Figure 257 Personal Certificate Import Wizard 6	417
Figure 258 Access the ZyXEL Device Via HTTPS	417
Figure 259 SSL Client Authentication	418
Figure 260 ZyXEL Device Secure Login Screen	418
Figure 261 Option to Enter Debug Mode	425
Figure 262 Boot Module Commands	426
Figure 263 Configuration Text File Format: Column Descriptions	437
Figure 264 Invalid Parameter Entered: Command Line Example	438
Figure 265 Valid Parameter Entered: Command Line Example	438
Figure 266 Internal SPTGEN FTP Download Example	439
Figure 267 Internal SPTGEN FTP Upload Example	439
Figure 268 Connecting a POTS Splitter	463
Figure 269 Connecting a Microfilter	464
Figure 270 ZyXEL Device with ISDN	464
Figure 271 Displaying Log Categories Example	479
Figure 272 Displaying Log Parameters Example	479
Figure 273 Ideal Setup	481
Figure 274 "Triangle Route" Problem	482
Figure 275 IP Alias	483
Figure 276 Gateways on the WAN Side	483

List of Tables

Table 1 ADSL Standards	42
Table 2 Front Panel LEDs	47
Table 3 Web Configurator Screens Summary	53
Table 4 Status Screen	56
Table 5 Status: Any IP Table	58
Table 6 Status: WLAN Status	59
Table 7 Status: VPN Status	60
Table 8 Status: Packet Statistics	61
Table 9 System General: Password	63
Table 10 Internet Access Wizard Setup: ISP Parameters	68
Table 11 Internet Connection with PPPoE	69
Table 12 Internet Connection with RFC 1483	70
Table 13 Internet Connection with ENET ENCAP	70
Table 14 Internet Connection with PPPoA	71
Table 15 Wireless LAN Setup Wizard 1	74
Table 16 Wireless LAN Setup Wizard 2	75
Table 17 Manually assign a WPA key	76
Table 18 Manually assign a WEP key	77
Table 19 Media Bandwidth Management Setup: Services	79
Table 20 Bandwidth Management Wizard: General Information	81
Table 21 Bandwidth Management Wizard: Configuration	82
Table 22 Internet Connection	91
Table 23 Advanced Internet Connection	93
Table 24 More Connections	95
Table 25 More Connections Edit	96
Table 26 More Connections Advanced Setup	98
Table 27 WAN Backup Setup	101
Table 28 WAN Backup Advanced Setup	103
Table 29 WAN Dial Backup Modem Setup	106
Table 30 LAN IP	115
Table 31 Advanced LAN Setup	116
Table 32 DHCP Setup	117
Table 33 LAN Client List	119
Table 34 LAN IP Alias	120
Table 35 Types of Encryption for Each Type of Authentication	125
Table 36 Additional Wireless Terms	127
Table 37 Wireless LAN: General	128
Table 38 Wireless No Security	129

Table 39 Wireless: Static WEP Encryption	130
Table 40 Wireless: WPA(2)-PSK	131
Table 41 Wireless: WPA(2)	133
Table 42 Wireless LAN: Advanced	134
Table 43 OTIST	136
Table 44 MAC Address Filter	140
Table 45 WMM QoS Priorities	141
Table 46 Commonly Used Services	143
Table 47 Wireless LAN: QoS	145
Table 48 Application Priority Configuration	146
Table 49 Multiple SSID Commands	149
Table 50 Multiple SSID Example Configuration	150
Table 51 DMZ	152
Table 52 NAT Definitions	157
Table 53 NAT Mapping Types	160
Table 54 NAT General	161
Table 55 Services and Port Numbers	162
Table 56 NAT Port Forwarding	164
Table 57 Port Forwarding Rule Setup	165
Table 58 Address Mapping Rules	166
Table 59 Edit Address Mapping Rule	167
Table 60 Common IP Ports	172
Table 61 ICMP Commands That Trigger Alerts	174
Table 62 Legal NetBIOS Commands	174
Table 63 Legal SMTP Commands	174
Table 64 Firewall: General	185
Table 65 Firewall Rules	186
Table 66 Firewall: Edit Rule	189
Table 67 Customized Services	190
Table 68 Firewall: Configure Customized Services	191
Table 69 Predefined Services	195
Table 70 Firewall: Anti Probing	198
Table 71 Firewall: Threshold	200
Table 72 Common Computer Virus Types	203
Table 73 Anti-Virus: Packet Scan	206
Table 74 Anti-Virus: Registration and Virus Information Update	208
Table 75 Content Filter: Keyword	212
Table 76 Content Filter: Schedule	213
Table 77 Content Filter: Trusted	213
Table 78 Content Access Control: General	216
Table 79 Control Access Control: General: Time Scheduling	218
Table 80 Content Access Control: General: Services	219
Table 81 Available Services	220

Table 82 Content Access Control: General: Web Site Filter	222
Table 83 Content Access Control: General: Diagnose	227
Table 84 Content Access Control: User Profiles	228
Table 85 Content Access Control: Online Status	229
Table 86 VPN and NAT	237
Table 87 AH and ESP	240
Table 88 VPN Setup	242
Table 89 VPN and NAT	244
Table 90 Local ID Type and Content Fields	246
Table 91 Peer ID Type and Content Fields	246
Table 92 Matching ID Type and Content Configuration Example	247
Table 93 Mismatching ID Type and Content Configuration Example	247
Table 94 Edit VPN Policies	248
Table 95 Advanced VPN Policies	255
Table 96 VPN: Manual Key	258
Table 97 VPN: SA Monitor	261
Table 98 VPN: Global Setting	262
Table 99 Telecommuters Sharing One VPN Rule Example	263
Table 100 Telecommuters Using Unique VPN Rules Example	264
Table 101 My Certificates	267
Table 102 My Certificate Import	270
Table 103 My Certificate Create	271
Table 104 My Certificate Details	274
Table 105 Trusted CAs	276
Table 106 Trusted CA Import	277
Table 107 Trusted CA Details	279
Table 108 Trusted Remote Hosts	281
Table 109 Trusted Remote Host Import	283
Table 110 Trusted Remote Host Details	285
Table 111 Directory Servers	287
Table 112 Directory Server Add	288
Table 113 Static Route	290
Table 114 Static Route Edit	291
Table 115 Application and Subnet-based Bandwidth Management Example	294
Table 116 Maximize Bandwidth Usage Example	296
Table 117 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example	296
Table 118 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example	297
Table 119 Bandwidth Management Priorities	297
Table 120 Media Bandwidth Management: Summary	298
Table 121 Bandwidth Management: Rule Setup	299
Table 122 Bandwidth Management Rule Configuration	301
Table 123 Services and Port Numbers	302
Table 124 Dynamic DNS	306

Table 125 Remote Management: WWW	311
Table 126 Remote Management: Telnet	312
Table 127 Remote Management: FTP	313
Table 128 SNMP Traps	315
Table 129 Remote Management: SNMP	316
Table 130 Remote Management: DNS	317
Table 131 Remote Management: ICMP	318
Table 132 TR-069 Commands	319
Table 133 Configuring UPnP	323
Table 134 System General Setup	334
Table 135 System Time Setting	336
Table 136 View Log	340
Table 137 Log Settings	341
Table 138 SMTP Error Messages	343
Table 139 Firmware Upgrade	345
Table 140 Maintenance Restore Configuration	348
Table 141 Diagnostic: General	351
Table 142 Diagnostic: DSL Line	352
Table 143 Troubleshooting Starting Up Your ZyXEL Device	353
Table 144 Troubleshooting the LAN	353
Table 145 Troubleshooting the WAN	354
Table 146 Troubleshooting Accessing the ZyXEL Device	355
Table 147 Device	365
Table 148 Firmware	366
Table 149 Classes of IP Addresses	390
Table 150 Allowed IP Address Range By Class	390
Table 151 "Natural" Masks	391
Table 152 Alternative Subnet Mask Notation	391
Table 153 Two Subnets Example	392
Table 154 Subnet 1	392
Table 155 Subnet 2	393
Table 156 Subnet 1	393
Table 157 Subnet 2	394
Table 158 Subnet 3	394
Table 159 Subnet 4	394
Table 160 Eight Subnets	395
Table 161 Class C Subnet Planning	395
Table 162 Class B Subnet Planning	396
Table 163 IEEE 802.11g	401
Table 164 Comparison of EAP Authentication Types	405
Table 165 Wireless Security Relational Matrix	407
Table 166 Certificates Commands	421
Table 167 Firewall Commands	427

Table 168 NetBIOS Filter Default Settings	434
Table 169 Abbreviations Used in the Example Internal SPTGEN Screens Table	439
Table 170 Menu 1 General Setup (SMT Menu 1)	440
Table 171 Menu 3 (SMT Menu 3)	440
Table 172 Menu 4 Internet Access Setup (SMT Menu 4)	443
Table 173 Menu 12 (SMT Menu 12)	445
Table 174 Menu 15 SUA Server Setup (SMT Menu 15)	449
Table 175 Menu 21.1 Filter Set #1 (SMT Menu 21.1)	451
Table 176 Menu 21.1 Filer Set #2, (SMT Menu 21.1)	454
Table 177 Menu 23 System Menus (SMT Menu 23)	459
Table 178 Menu 24.11 Remote Management Control (SMT Menu 24.11)	460
Table 179 Command Examples	460
Table 180 System Maintenance Logs	465
Table 181 System Error Logs	466
Table 182 Access Control Logs	466
Table 183 TCP Reset Logs	467
Table 184 Packet Filter Logs	467
Table 185 ICMP Logs	468
Table 186 CDR Logs	468
Table 187 PPP Logs	468
Table 188 UPnP Logs	469
Table 189 Content Filtering Logs	469
Table 190 Attack Logs	470
Table 191 IPSec Logs	471
Table 192 IKE Logs	471
Table 193 PKI Logs	474
Table 194 Certificate Path Verification Failure Reason Codes	475
Table 195 802.1X Logs	476
Table 196 ACL Setting Notes	477
Table 197 ICMP Notes	477
Table 198 Syslog Logs	478
Table 199 RFC-2408 ISAKMP Payload Types	478

Preface

Congratulations on your purchase of the P-662H/HW-D series 802.11g Wireless ADSL 2+ 4-port Gateway. P-662H-D has a 4-port switch that allows you to connect up to 4 computers to the ZyXEL Device without purchasing a switch/hub. P-662HW-D comes with built-in IEEE 802.11g wireless capability allowing wireless connectivity.

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

About This User's Guide

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

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

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choice.
- Mouse action sequences are denoted using a right angle bracket (>). For example, “In Windows, click **Start > Settings > Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.
- The P-662HW-D and P-662H-D may be referred to as the “ZyXEL Device” in this User’s Guide.











Related Documentation

- Supporting Disk
Refer to the included CD for support documents.
- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains connection information and instructions on getting started.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

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

Graphics Icons Key

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

CHAPTER 1

Getting To Know Your ZyXEL Device

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

1.1 Introducing the ZyXEL Device

Your ZyXEL Device integrates high-speed 10/100Mbps auto-negotiating LAN interface(s) and a high-speed ADSL port into a single package. The ZyXEL Device is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks.

In the ZyXEL Device product name, “H” denotes an integrated 4-port hub and “W” denotes wireless functionality. The P-662HW-Dx has an embedded mini-PCI module for 802.11g+ Wireless LAN connectivity.

Note: All wireless features in this guide pertain to the P-662HW-Dx series only.

Models ending in “1”, for example P-662HW-D1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3” denote a device that works over ISDN (Integrated Services Digital Network). Models ending in “7” denote a device that works over T-ISDN (UR-2).

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

1.1.1 Features of the ZyXEL Device

The following sections describe the features of the ZyXEL Device.

Note: See the product specifications in the appendix for detailed features and standards support.

High Speed Internet Access

The ZyXEL Device is an ADSL router compatible with the ADSL/ADSL2/ADSL2+ standards. Maximum data rates attainable for each standard are shown in the next table.

Table 1 ADSL Standards

DATA RATE STANDARD	UPSTREAM	DOWNSTREAM
ADSL	832 kbps	8Mbps
ADSL2	3.5Mbps	12Mbps
ADSL2+	3.5Mbps	24Mbps

Note: If your ZyXEL Device does not support Annex M, the maximum ADSL2/2+ upstream data rate is 1.2 Mbps. ZyXEL Devices which work over ISDN do not support Annex M.

The standard your ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, line quality, etc.

Zero Configuration Internet Access

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

Any IP

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

Firewall

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

Content Filtering

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

LAN/DMZ Interface

The ZyXEL Device provides a LAN port that can function as a virtual DeMilitarized Zone (DMZ) port. Public servers (Web, FTP, etc.) attached to the DMZ port are visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death) and can also be accessed from the secure LAN.

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 fully interoperable with other IPSec-based VPN products.

Traffic Redirect

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

Media Bandwidth Management

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

Universal Plug and Play (UPnP)

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

PPPoE (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the ZyXEL Device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers. The ZyXEL Device also includes PPPoE idle time-out (the PPPoE connection terminates after a period of no traffic that you configure) and PPPoE Dial-on-Demand (the PPPoE connection is brought up only when an Internet access request is made).

Network Address Translation (NAT)

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

Dynamic DNS Support

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

DHCP

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

IP Alias

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

IP Policy Routing (IPPR)

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

Packet Filters

The ZyXEL Device's packet filtering functions allows added network security and management.

Housing

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

TR-069 Compliance

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

1.1.1.1 P-662HW Wireless Features

Wireless LAN

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

Note: The P-662HW may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

Wi-Fi Protected Access

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

Wireless g+

Wireless g+ technology allows super fast transmission rates (actual speed depends on environment) among Wireless g+ enabled access points and wireless clients.

Antenna

The ZyXEL Device is equipped with a detachable SMA 5dBi high gain Antenna to provide clear radio signal between the wireless stations and the access points.

Wireless LAN MAC Address Filtering

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

WEP Encryption

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

OTIST (One Touch Intelligent Security Technology)

OTIST allows your ZyXEL Device to assign its ESSID and security settings (WEP or WPA-PSK) to the ZyXEL wireless adapters that support OTIST and are within transmission range. The ZyXEL wireless adapters must also have OTIST enabled.

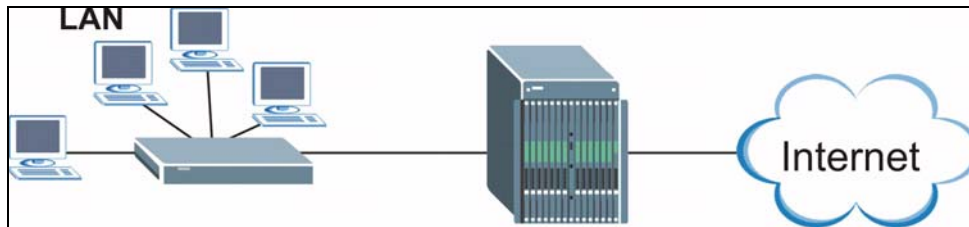
1.1.2 Applications for the ZyXEL Device

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

1.1.2.1 Internet Access

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

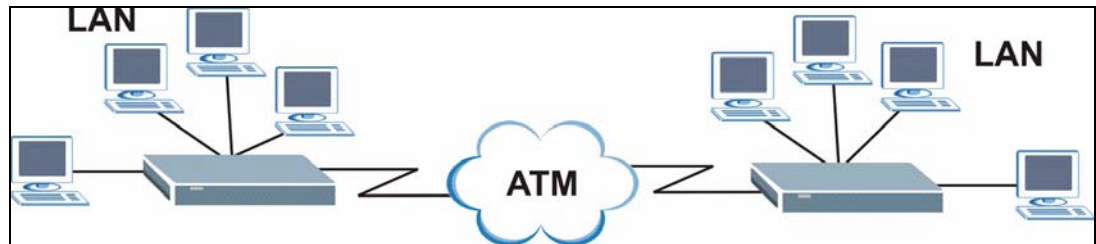
Figure 1 ZyXEL Device Internet Access Application



1.1.2.2 LAN to LAN Application

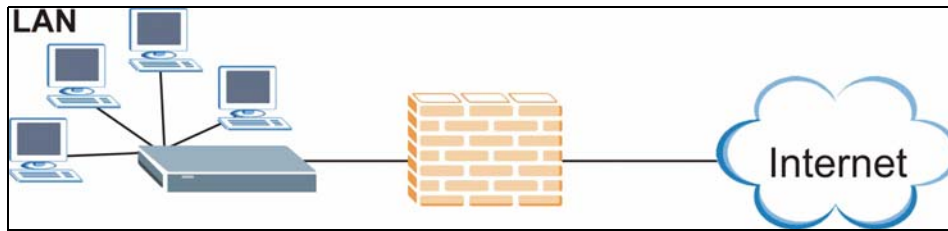
You can use the ZyXEL Device to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application example for the ZyXEL Device is shown as follows.

Figure 2 ZyXEL Device LAN-to-LAN Application Example

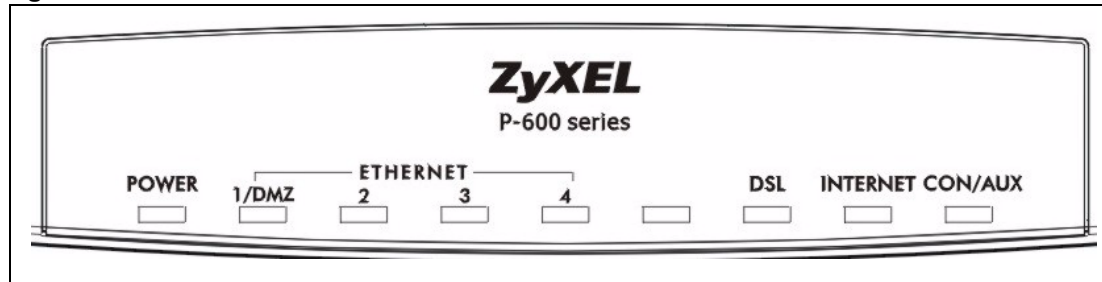
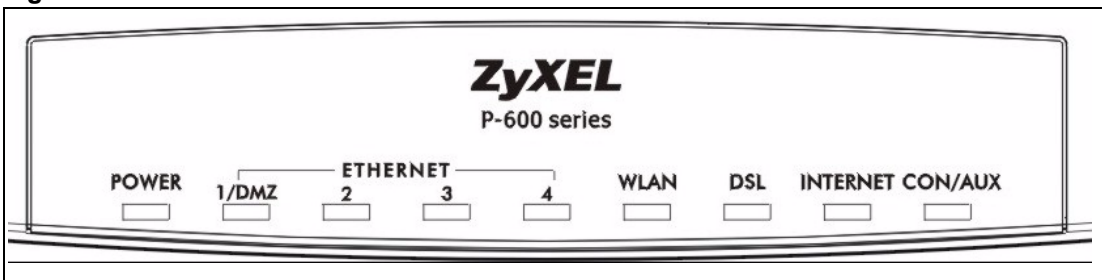


1.1.3 Firewall for Secure Broadband Internet Access

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

Figure 3 Firewall Application

1.1.4 Front Panel LEDs

Figure 4 P-662H Front Panel**Figure 5** P-662HW Front Panel

The following table describes the Lights.

Table 2 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting or performing diagnostics.
	Red	On	Post (Power On Self Test) failure or the device has malfunctioned.
		Off	The system is not receiving power.
LAN 1-4	Green	On	The ZyXEL Device has a successful 10/100Mb Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
	None	Off	The LAN is not connected.

Table 2 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
WLAN (P-662HW only)	Green	On	The ZyXEL Device is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The ZyXEL Device is sending/receiving data through the wireless LAN.
	None	Off	The wireless LAN is not ready or has failed.
DSL/ACT	Green	On	The ZyXEL Device has a successful DSL connection.
		Blinking	The DSL is attempting to synchronize with the ZyXEL Device.
		Off	The system is not receiving power or there is no DSL connection.
INTERNET	Green	On	The ZyXEL Device is connected with no traffic detected.
		Blinking	The ZyXEL Device is sending/receiving data.
	Red	On	The ZyXEL Device failed to authenticate.
		Off	The DSL line is down.
CON/AUX	Green	On	The CON/AUX switch is set to CON, the CON/AUX port is connected to a management computer and someone is logged into the ZyXEL Device.
		Off	The CON/AUX link is not ready, or has failed.
	Amber	On	The CON/AUX switch is set to AUX and the CON/AUX port has an Internet connection through a dial-up modem.
		Blinking	The CON/AUX switch is set to AUX and the CON/AUX port is sending or receiving data through a dial-up modem or ISDN TA.

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

CHAPTER 2

Introducing the Web Configurator

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

2.1 Web Configurator Overview

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

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

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

See the chapter on troubleshooting if you need to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

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

- 1** Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
- 2** Prepare your computer/computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
- 3** Launch your web browser.
- 4** Type "192.168.1.1" as the URL.
- 5** A window displays as shown. Enter the default admin password **admin** to configure the wizards and the advanced features or the default user password **user** to view the status

only. Click **Login** to proceed to a screen asking you to change your password or click **Cancel** to revert to the default password.

Figure 6 Password Screen

The image shows the ZyXEL password screen. At the top is the ZyXEL logo. Below it, 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 input field are two buttons: "Login" and "Cancel".

- 6** If you entered the user password, skip the next two steps and refer to [Section 2.4.2 on page 55](#) for more information about the **Status** screen.

If you entered the admin password, it is highly recommended you change the default admin password! Enter a new password between 1 and 30 characters, 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.

Note: If you do not change the password at least once, the following screen appears every time you log in with the admin password.

Figure 7 Change Password at Login

The image shows the ZyXEL "Change Password at Login" 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 input fields are two buttons: "Apply" and "Ignore".

- 7** It is highly recommended you replace the factory default certificate by creating your own unique certificate based on your ZyXEL Device's MAC address. Click **Apply** to create the certificate, alternatively click **Ignore** to proceed to the next menu if you do not want to replace the certificate now.

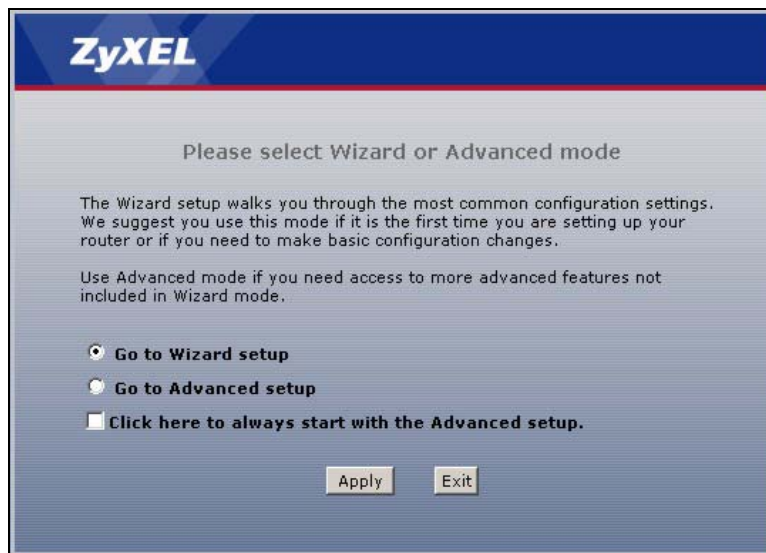
Note: If you do not replace the certificate, the following screen appears every time you log in.

Figure 8 Replace Factory Default Certificate



- 8** Select **Go to Wizard setup** and click **Apply** to display the wizard main screen. Otherwise, select **Go to Advanced setup** and click **Apply** to display the **Status** screen.

Figure 9 Select a Mode



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

2.3 Resetting the ZyXEL Device

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

2.3.1 Using the Reset Button

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Press the **RESET** button for 10 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts.

You can also use the **RESET** button to:

- Activate/Deactivate the wireless network - by pressing the **RESET** button for 1 second.
- Start OTIST - by pressing the **RESET** button for 3 seconds.

2.4 Navigating the Web Configurator

We use the P-662HW-D1 web screens in this guide as an example. Screens vary slightly for different ZyXEL Device models.

2.4.1 Navigation Panel

After you enter the admin password, use the sub-menus on the navigation panel to configure ZyXEL Device features. The following table describes the sub-menus.

Figure 10 Web Configurator: Main Screen

The screenshot shows the ZyXEL Web Configurator interface. On the left is a navigation panel with a tree view containing the following sub-menus:

- Network
 - Remote Node
 - WAN
 - LAN
 - Wireless LAN
 - DMZ
 - NAT
- Security
- Advanced
- Maintenance
 - System
 - Logs
 - Tools
 - Diagnostic

The main content area is titled "Status" and is divided into several sections:

- Device Information:** Host Name, Model Number (P662HW-D1), MAC Address, ZyNOS Firmware Version (V3.40(AGZ.0)b1 | 01/17/2006), WAN Information (DSL Mode: NORMAL, IP Address: 0.0.0.0, Subnet Mask: 0.0.0.0, Default Gateway: 0.0.0.0, VPI/VCI: 0/33), LAN Information (IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, DHCP: Server), WLAN Information (SSID: Wireless, Channel: 0, WEP: Disable), and Security (Enabled, Disabled, Disabled).
- System Status:** System Uptime, Current CPU Usage, System Memory Usage, CPU Usage, and Memory Usage (29%).
- Interface Status:** A table showing the status of various interfaces.

Interface	Status	Rate
DSL	Down	0 kbps / 0 kbps
LAN	Up	100M/Full DuplexInActive
WLAN	InActive	N/A
DMZ	100M/Full DuplexInActive	N/A
- Summary:** Links to AnyIP Table, Bandwidth Status, Packet Statistics, WLAN Status, and VPN Status.

Annotations in the image include a red arrow pointing to a Logout icon in the top right corner with a text box stating: "Click the Logout icon at any time to exit the web configurator." and another text box pointing to the navigation panel stating: "Use submenus to configure ZyXEL Device".


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

Table 3 Web Configurator Screens Summary



LINK/ICON	SUB-LINK	FUNCTION
Wizard 	INTERNET/WIRELESS SETUP	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
	BANDWIDTH MANAGEMENT SETUP	Use these screens to limit bandwidth usage by application or packet type.
Logout 		Click this icon to exit the web configurator.
Status		This screen shows the ZyXEL Device's general device, system and interface status information. Use this screen to access the summary statistics tables.
Network		
Remote Node		Use this screen to configure placing calls to a remote gateway.
WAN	Internet Access Setup	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	WAN Backup Setup	Use this screen to configure your traffic redirect properties and WAN backup settings.
LAN	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
	IP Alias	Use this screen to partition your LAN interface into subnets.
Wireless LAN (Wireless devices only)	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	OTIST	This screen allows you to assign wireless clients the ZyXEL Device's wireless security settings.
	MAC Filter	Use this screen to configure the ZyXEL Device to block access to devices or block the devices from accessing the ZyXEL Device.
	QoS	WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of the individual and applications.
DMZ	DMZ	Use this screen to create and enable a DMZ port.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the ZyXEL Device.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to change your anti-probing settings.

Table 3 Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
	Threshold	Use this screen to configure the threshold for DoS attacks.
Anti Virus	Packet Scan	Use this screen to change your Packet Scan settings.
	Registration	Use this screen to register, activate or update your anti-virus services.
Content Filter	Keyword	Use this screen to block sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the ZyXEL Device to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering on your ZyXEL Device.
Content Access Control	General	Use this screen to activate Content Access Control and create user groups.
	User Profile	Use this screen to create user accounts.
	Online Status	Use this screen to view the online status.
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		Use this screen to configure IP static routes.
Bandwidth MGMT	Summary	Use this screen to enable 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		Use this screen to set up dynamic DNS.

Table 3 Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	ICMP	Use this screen to change your anti-probing settings.
UPnP		Use this screen to enable UPnP on the ZyXEL Device.
Maintenance		
System	General	This screen contains administrative and system-related information and also allows you to change your password.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your ZyXEL Device's log settings.
Tools	Firmware	Use this screen to upload firmware to your ZyXEL Device.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your ZyXEL Device.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	General	These screens display information to help you identify problems with the ZyXEL Device general connection.
	DSL Line	These screens display information to help you identify problems with the DSL line.

2.4.2 Status Screen

The following summarizes how to navigate the web configurator from the **Status** screen. Some fields or links are not available if you entered the user password in the login password screen (see [Figure 6 on page 50](#)).

Figure 11 Status Screen



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

Table 4 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Apply	Click this button to refresh the status screen statistics.
Device Information	
Host Name	This is the System Name you enter in the Maintenance, System, General screen. It is for identification purposes.
Model Number	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL Firmware Version	This is the DSL firmware version associated with your ZyXEL Device.
WAN Information	
DSL Mode	This is the standard that your ZyXEL Device is using.
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.

Table 4 Status Screen

LABEL	DESCRIPTION
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the Wizard or WAN screen.
LAN Information	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - Server , Relay or None .
WLAN Information (wireless devices only)	
SSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN.
Channel	This is the channel number used by the ZyXEL Device now.
WEP	This displays the status of WEP data encryption.
Security	
Firewall	This displays whether or not the ZyXEL Device's firewall is activated.
Content Filter	This displays whether or not the ZyXEL Device's content filtering is activated.
Anti Virus	This displays whether or not the ZyXEL Device's anti-virus is activated.
System Status	
System Uptime	This is the total time the ZyXEL Device has been on.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This number shows how many kilobytes of the heap memory the ZyXEL Device is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall. The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Memory Usage	This number shows the ZyXEL Device's total heap memory (in kilobytes). The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Interface Status	
Interface	This displays the ZyXEL Device port types.
Status	This field displays Down (line is down), Up (line is up or connected) if you're using Ethernet encapsulation and Down (line is down), Up (line is up or connected), Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE encapsulation. For the WLAN port, it displays Active when WLAN is enabled or Inactive when WLAN is disabled. For the DMZ port, it displays the port speed, duplex mode and whether the port is Active or Inactive .
Rate	For the LAN ports, this displays the port speed and duplex setting. For the WAN port, it displays the downstream and upstream transmission rate. For the WLAN port, it displays the transmission rate when WLAN is enabled or N/A when WLAN is disabled. For the DMZ port, it displays the transmission rate when DMZ is enabled or N/A when DMZ is disabled.

Table 4 Status Screen

LABEL	DESCRIPTION
Summary	
Any IP Table	Use this screen to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the ZyXEL Device.
WLAN Status (wireless devices only)	This screen displays the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device.
Bandwidth Status	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Packet Statistics	Use this screen to view port status and packet specific statistics.
VPN Status	Use this screen to view VPN status and settings.

2.4.3 Status: Any IP Table

Click the **Any IP Table** hyperlink in the **Status** screen. The Any IP table shows current read-only information (including the IP address and the MAC address) of all network devices that use the Any IP feature to communicate with the ZyXEL Device.

Figure 12 Status: Any IP Table

Any IP Table		
#	IP Address	MAC Address
1	255.255.255.255	11:22:33:44:55:66

Refresh

The following table describes the labels in this screen.

Table 5 Status: Any IP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address of the network device.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed IP address. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click Refresh to update this screen.

2.4.4 Status: WLAN Status

Click the **WLAN Status** hyperlink in the **Status** screen to view the wireless stations that are currently associated to the ZyXEL Device.

Figure 13 Status: WLAN Status

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

Refresh

The following table describes the labels in this screen.

Table 6 Status: 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 P-662H/HW-Dx.
Refresh	Click Refresh to reload this screen.

2.4.5 Status: Bandwidth Status

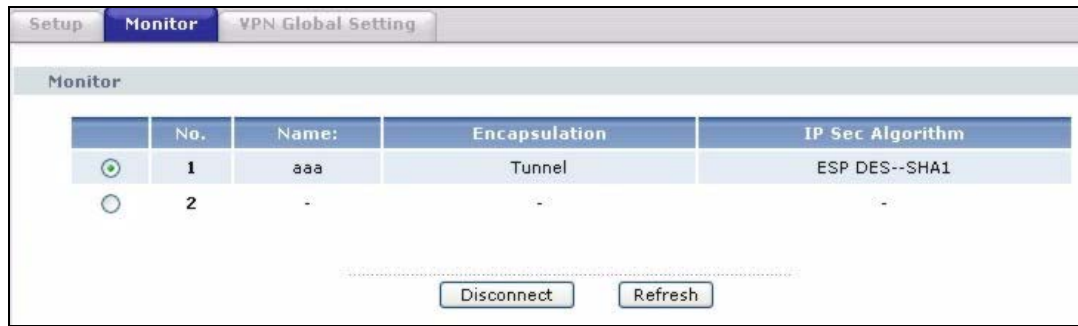
Select the **Bandwidth Status** hyperlink in the **Status** screen. View the bandwidth usage of the LAN, WAN and WLAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the orange color represents the percentage of bandwidth in use.

Figure 14 Status: Bandwidth Status

Monitor		
LAN		
To LAN Interface		
www	<div style="width: 0%; background-color: gray; height: 15px;"></div>	0 / 100000 kbps
Telnet	<div style="width: 0%; background-color: gray; height: 15px;"></div>	0 / 100000 kbps

2.4.6 Status: VPN Status

Click the **VPN Status** hyperlink in the **Status** screen. The **VPN Status** shows the current status of any VPN tunnels the ZyXEL Device has negotiated.

Figure 15 Status: VPN Status

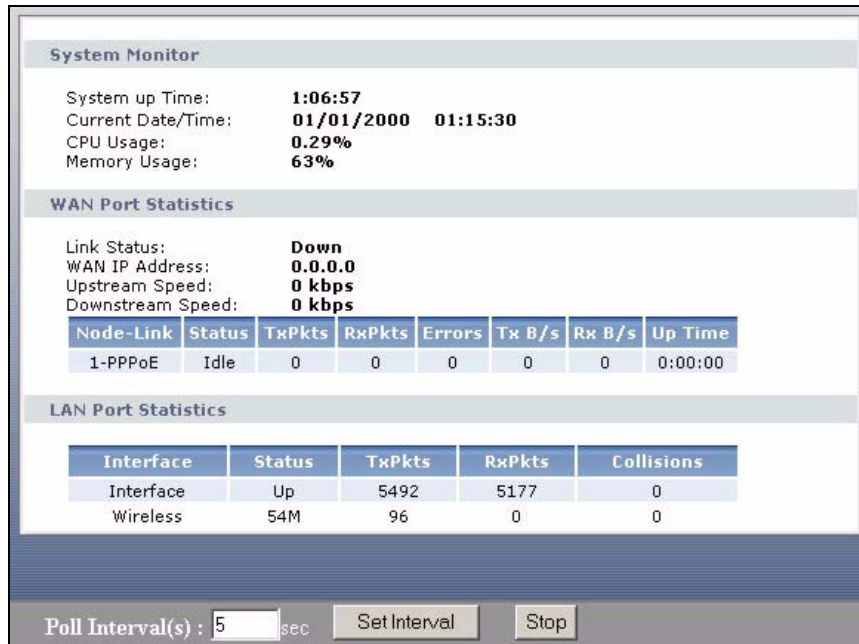
The following table describes the labels in this screen.

Table 7 Status: VPN Status

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

2.4.7 Status: Packet Statistics

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

Figure 16 Status: Packet Statistics

The following table describes the fields in this screen.

Table 8 Status: Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
LAN or WAN Port Statistics	
Link Status	This is the status of your WAN link.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Interface	This field displays the type of port.
Status	This field displays Down (line is down), Up (line is up or connected) if you're using Ethernet encapsulation and Down (line is down), Up (line is up or connected), Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE encapsulation. For the WLAN port, it displays the transmission rate when WLAN is enabled or N/A when WLAN is disabled.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.

Table 8 Status: Packet Statistics (continued)

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

2.4.8 Changing Login Password

It is highly recommended that you periodically change the password for accessing the ZyXEL Device. If you didn't change the default one after you logged in or you want to change to a new password again, then click **Maintenance > System** to display the screen as shown next.

Figure 17 System General

The screenshot shows the 'System General' configuration page. It features two tabs: 'General' and 'Time Setting'. The 'System Setup' section includes fields for 'System Name', 'Domain Name', and 'Administrator Inactivity Timer' (set to 60 minutes). The 'Password' section is highlighted with a red rounded rectangle and contains fields for 'User Password' (New Password, Retype to confirm) and 'Admin Password' (Old Password, New Password, Retype to confirm). A 'Caution' message is displayed below the password fields, and 'Apply' and 'Cancel' buttons are at the bottom.

The following table describes the fields in this screen.

Table 9 System General: Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 3

Wizard Setup for Internet Access

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


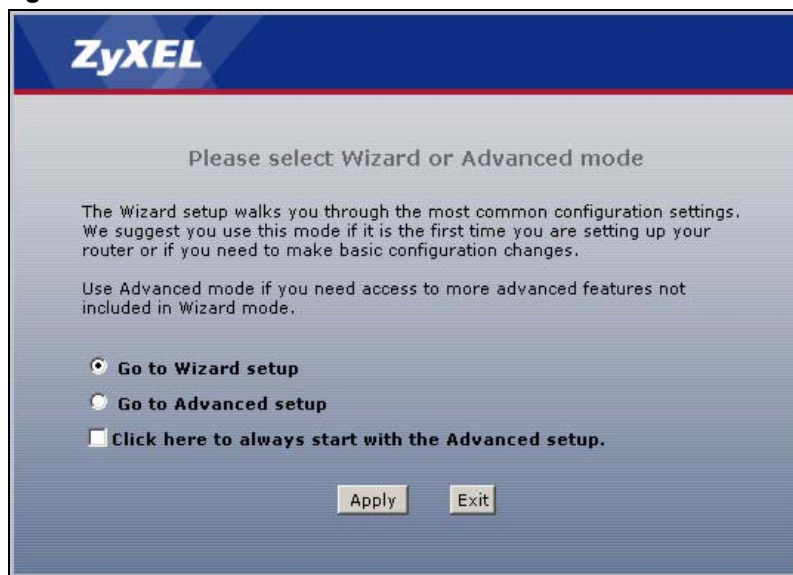
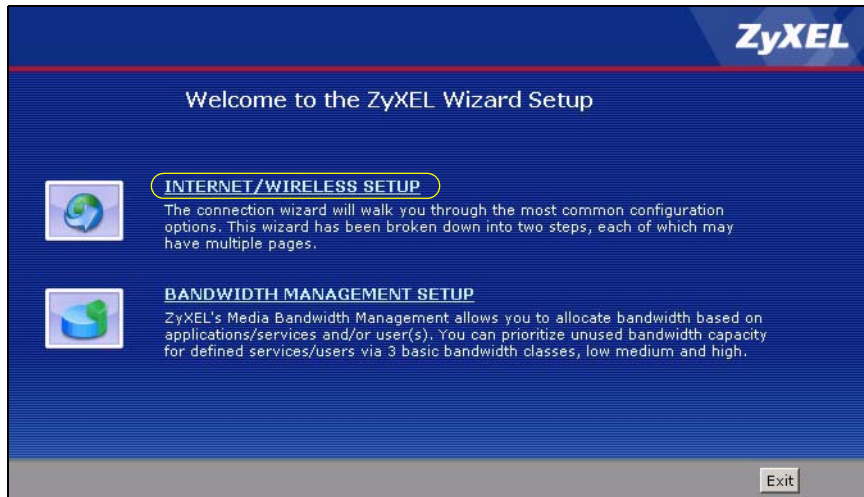
- 1 After you enter the admin password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon () in the top right corner of the web configurator to display the wizard main screen.

Figure 18 Select a Mode



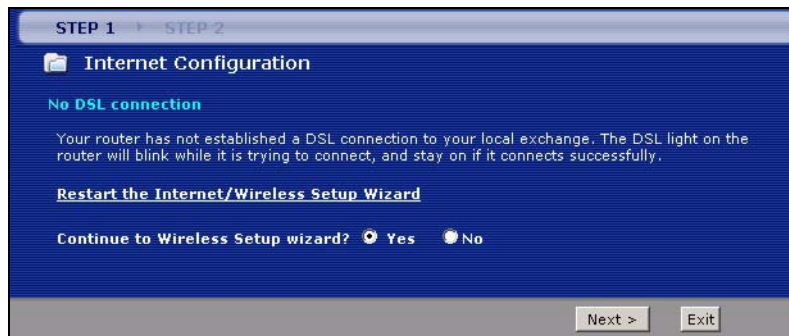
- 2 Click **INTERNET/WIRELESS SETUP** to configure the system for Internet access and wireless connection.

Figure 19 Wizard: Welcome

3 The wizard attempts to detect which WAN connection type you are using.

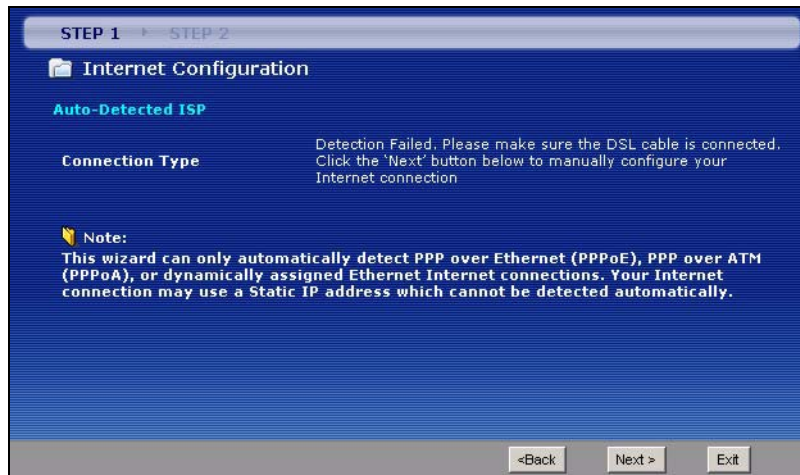
If the wizard detects your connection type and your ISP uses PPPoE or PPPoA, go to [Section 3.2.1 on page 67](#). The screen varies depending on the connection type you use.

If the wizard does not detect a connection type and the following screen appears (see [Figure 20 on page 66](#)), check your hardware connections and click **Restart the Internet/Wireless Setup Wizard** to have the ZyXEL Device detect your connection again.

Figure 20 Auto Detection: No DSL Connection

If the wizard still cannot detect a connection type and the following screen appears (see [Figure 21 on page 67](#)), click **Next** and refer to [Section 3.2.2 on page 67](#) on how to configure the ZyXEL Device for Internet access manually.

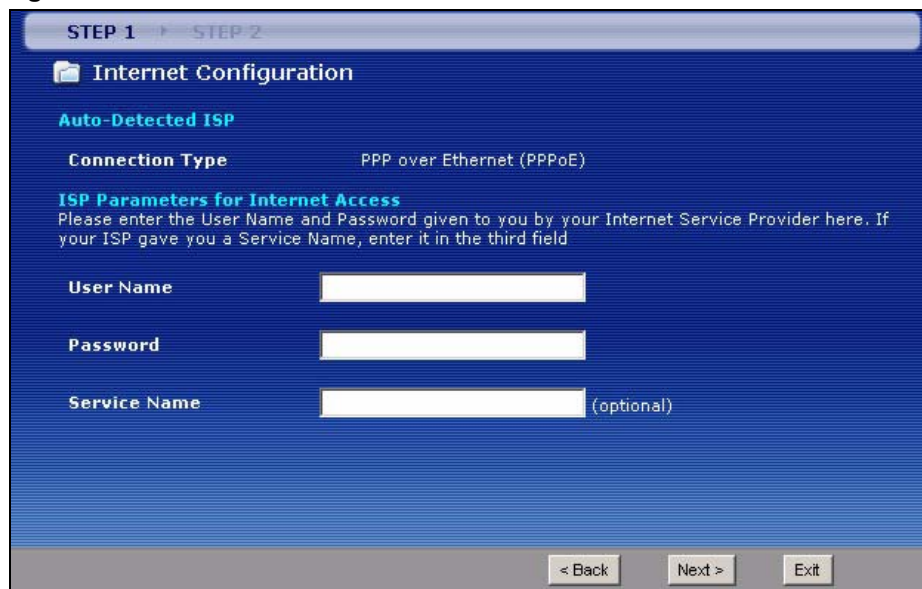
Figure 21 Auto Detection: Failed



3.2.1 Automatic Detection

- 1 If you have a PPPoE or PPPoA connection, a screen displays prompting you to enter your Internet account information. Enter the username, password and/or service name exactly as provided.
- 2 Click **Next** and see [Section 3.3 on page 72](#) for wireless connection wizard setup.

Figure 22 Auto-Detection: PPPoE



3.2.2 Manual Configuration

- 1 If the ZyXEL Device fails to detect your DSL connection type, enter the Internet access information given to you by your ISP exactly in the wizard screen. If not given, leave the fields set to the default.

Figure 23 Internet Access Wizard Setup: ISP Parameters

The following table describes the fields in this screen.

Table 10 Internet Access Wizard Setup: ISP Parameters

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

- 2 The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue. See [Section 3.3 on page 72](#) for wireless connection wizard setup

Figure 24 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 11 Internet Connection with PPPoE

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

Figure 25 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 12 Internet Connection with RFC 1483

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

Figure 26 Internet Connection with ENET ENCAP



The following table describes the fields in this screen.

Table 13 Internet Connection with ENET ENCAP

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

Table 13 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 Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Exit	Click Exit to close the wizard screen without saving your changes.

Figure 27 Internet Connection with PPPoA

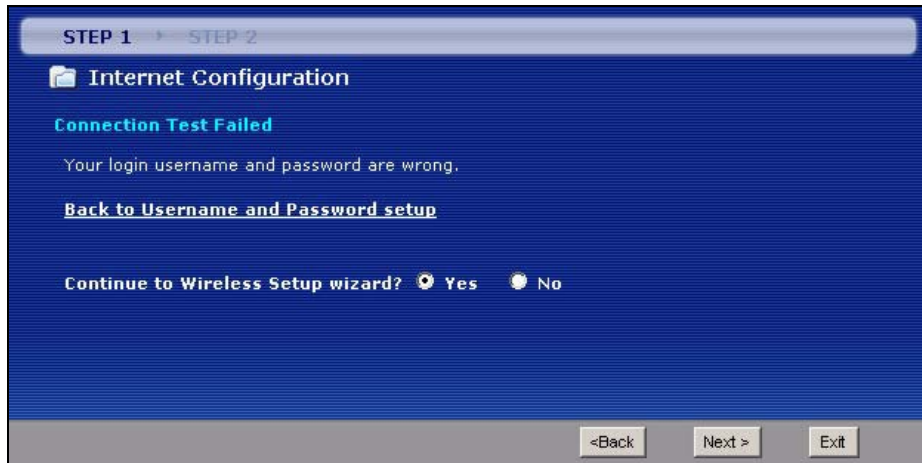
The screenshot shows a blue-themed wizard screen. At the top, it says 'STEP 1' and 'STEP 2'. Below that is the title 'Internet Configuration'. Underneath, it says 'ISP Parameters for Internet Access' and 'Please enter the User Name and Password given to you by your Internet Service Provider here'. There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

The following table describes the fields in this screen.

Table 14 Internet Connection with PPPoA

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

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

Figure 28 Connection Test Failed-1

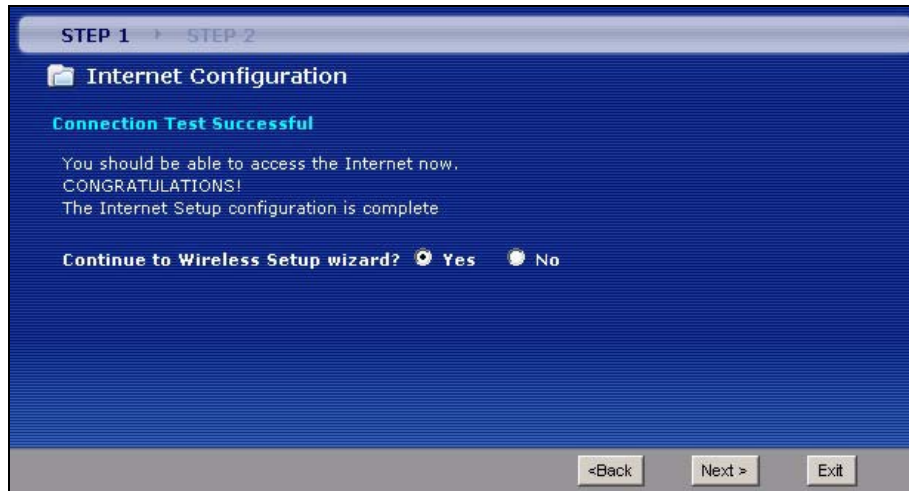
- If the following screen displays, check if your account is activated or click **Restart the Internet/Wireless Setup Wizard** to verify your Internet access settings.

Figure 29 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 30 Connection Test Successful

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

Figure 31 Wireless LAN Setup Wizard 1

The following table describes the labels in this screen.

Table 15 Wireless LAN Setup Wizard 1

LABEL	DESCRIPTION
Active	Select the check box to turn on the wireless LAN. Note: You can also activate the wireless LAN by pressing the RESET button for 1 second.
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. Note: You can start OTIST by pressing the RESET button for 3 seconds.
Setup Key	Type an OTIST Setup Key of up to eight ASCII characters in length. Be sure to use the same OTIST Setup Key on the ZyXEL Device and wireless clients.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

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

Figure 32 Wireless LAN Setup Wizard 2

The screenshot shows the 'Wireless LAN' configuration screen. At the top, it indicates 'STEP 1' and 'STEP 2'. Below the title, there are three main sections: 'Network Name (SSID)' with a text input field containing 'ZyXEL', 'Channel Selection' with a dropdown menu showing 'Channel-06 2437MHz', and 'Security' with a dropdown menu showing 'Manually assign a WPA-PSK key'. Each section has a brief explanatory text below it. At the bottom of the screen, there are three buttons: '<Back', 'Next >', and 'Exit'.

The following table describes the labels in this screen.

Table 16 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 Automatically assign a WPA key 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 Enable OTIST . See Section 3.3.1 on page 75 for more information. Select Manually assign a WPA-PSK key to configure a Pre-Shared Key (WPA-PSK). Choose this option only if your wireless clients support WPA. See Section 3.3.2 on page 75 for more information. Select Manually assign a WEP key to configure a WEP Key. See Section 3.3.3 on page 76 for more information. Select Disable wireless security to have no wireless LAN security configured and your network is accessible to any wireless networking device that is within range.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

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

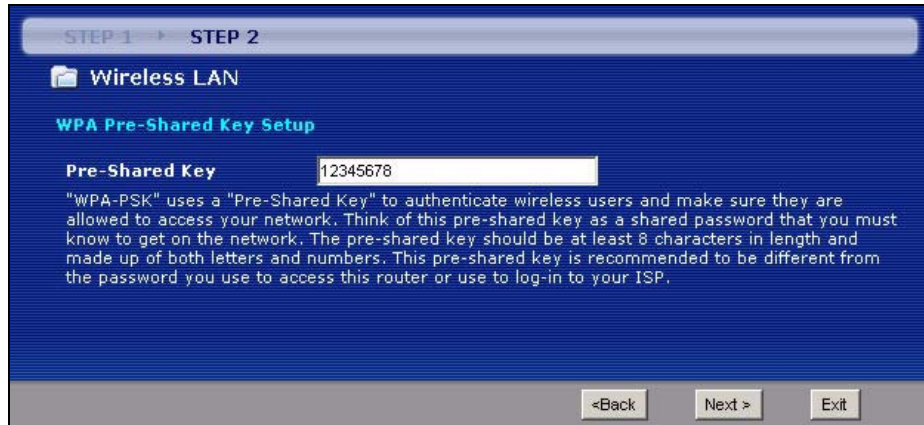
- 4 This screen varies depending on the security mode you selected in the previous screen. Fill in the field (if available) and click **Next**.

3.3.1 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-PSK key

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

Figure 33 Manually assign a WPA key

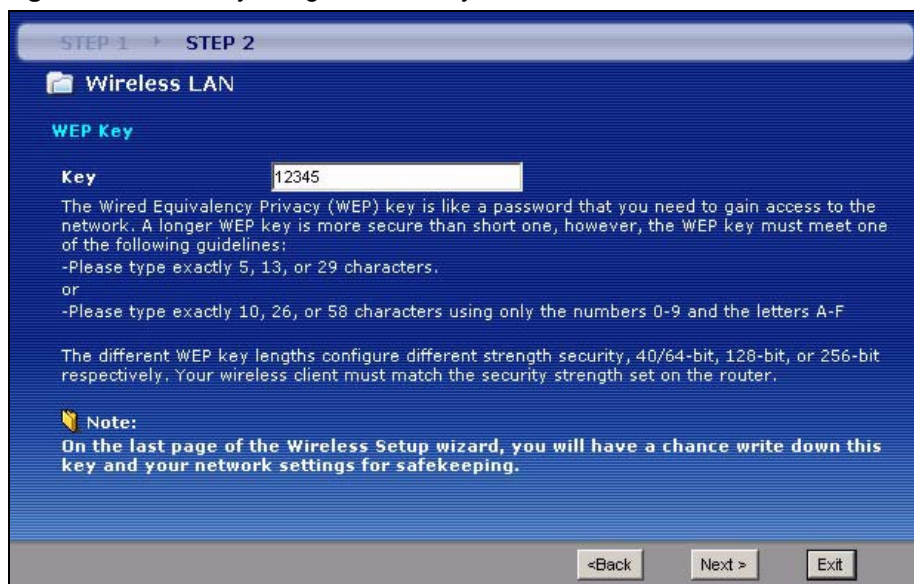
The following table describes the labels in this screen.

Table 17 Manually assign a WPA key

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

3.3.3 Manually assign a WEP key

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

Figure 34 Manually assign a WEP key

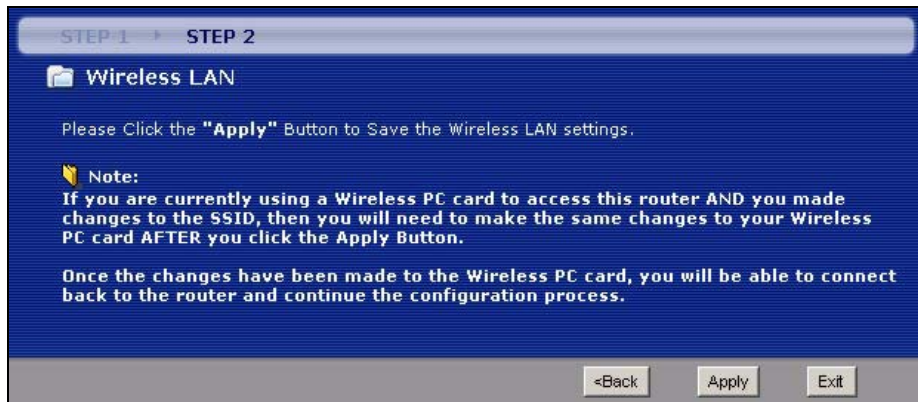
The following table describes the labels in this screen.

Table 18 Manually assign a WEP key

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

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

Figure 35 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.

Figure 36 Internet Access and WLAN Wizard Setup Complete

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

CHAPTER 4

Bandwidth Management Wizard

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

4.1 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.

4.2 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 19 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 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	The purpose of the TELNET Protocol is to provide a fairly general, bi-directional, eight-bit byte oriented communications facility. It is typically used to provide user oriented command line login sessions between hosts on the Internet. Telnet uses port number 23.
NetMeeting (H.323)	H.323 is an umbrella recommendation from the ITU-T, that defines the protocols to provide audio-visual communication sessions on any packet network.

Table 19 Media Bandwidth Management Setup: Services (continued)

SERVICE	DESCRIPTION
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)	H.323 is an umbrella recommendation from the ITU-T, that defines the protocols to provide audio-visual communication sessions on any packet network.
TFTP	Trivial File Transfer Protocol (TFTP) is a very simple file transfer protocol, with the functionality of a very basic form of FTP. It is used to transfer small files between hosts on a network, such as when a remote X Window System terminal or any other thin client boots from a network host or server. TFTP is transported primarily over UDP.

4.3 Bandwidth Management Wizard Setup


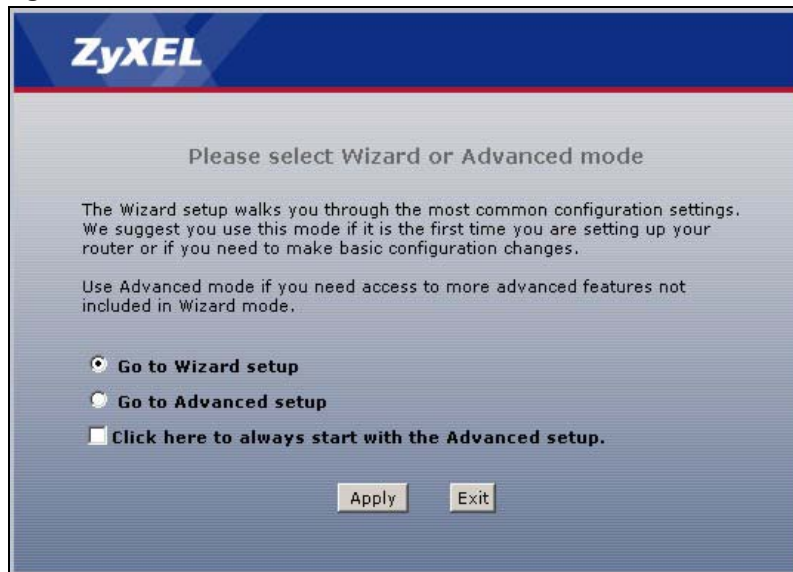
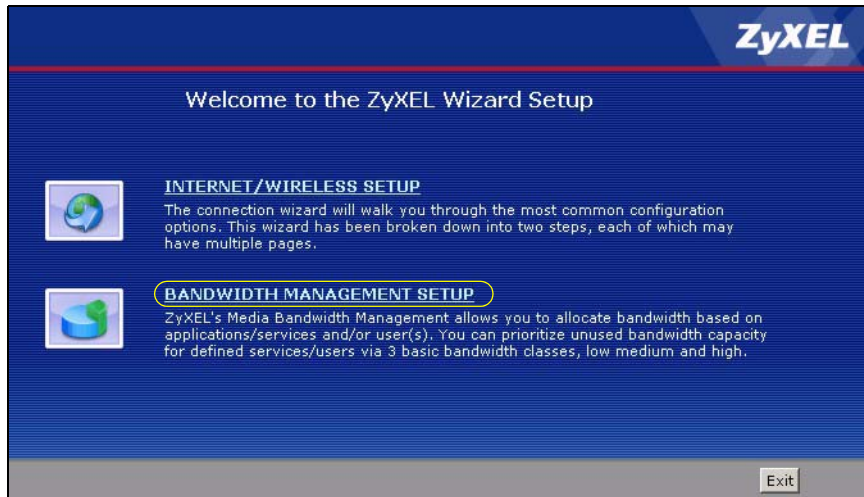
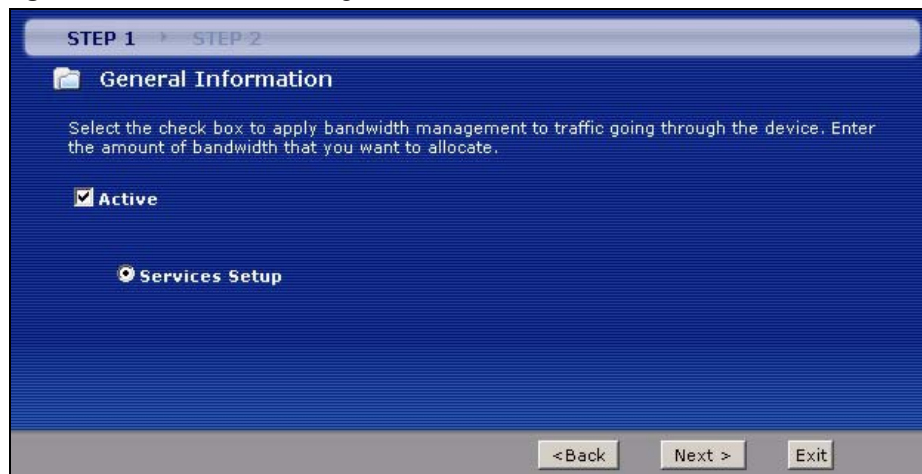
- 1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon () in the top right corner of the web configurator to display the wizard main screen.

Figure 37 Select a Mode

- 2 Click **BANDWIDTH MANAGEMENT SETUP** to configure the system for Internet access and wireless connection.

Figure 38 Wizard: Welcome

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

Figure 39 Bandwidth Management Wizard: General Information

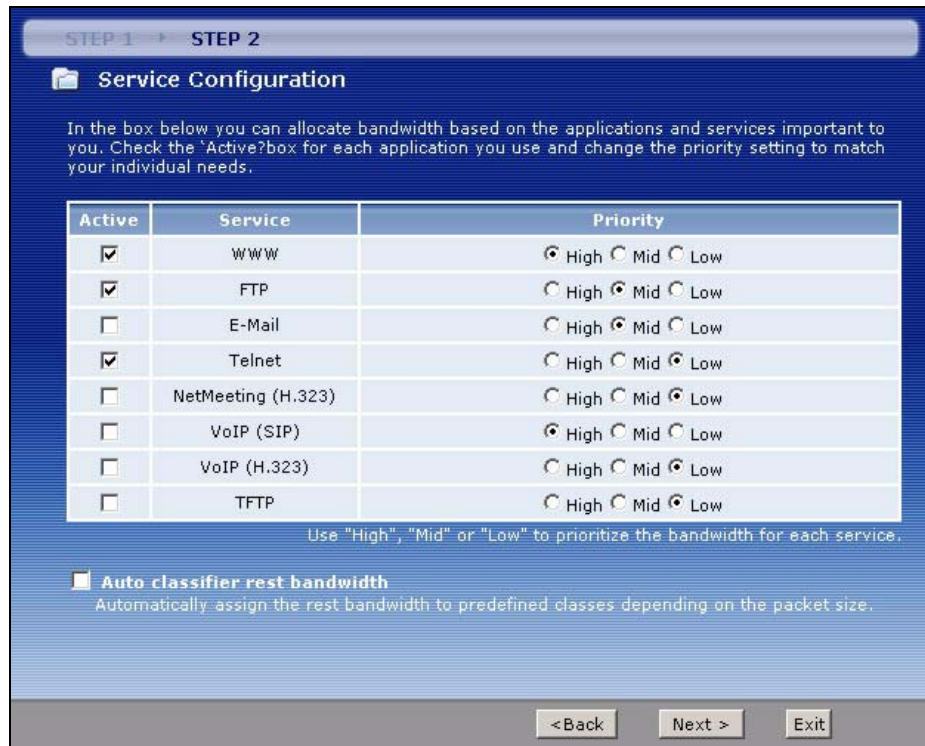
The following fields describe the label in this screen.

Table 20 Bandwidth Management Wizard: General Information

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

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

Figure 40 Bandwidth Management Wizard: Configuration



The following table describes the labels in this screen.

Table 21 Bandwidth Management Wizard: Configuration

LABEL	DESCRIPTION
Active	Select an entry's Active check box to turn on bandwidth management for the service/application.
Service	These fields display the services names.
Priority	Select High , Mid or Low priority for each service to have your ZyXEL Device use a priority for traffic that matches that service. A service with High priority is given as much bandwidth as it needs. If you select services as having the same priority, then bandwidth is divided equally amongst those services. Services not specified in bandwidth management are allocated bandwidth after all specified services receive their bandwidth requirements. If the rules set up in this wizard are changed in Advanced > Bandwidth MGMT > Rule Setup , then the service priority radio button will be set to User Configured . The Advanced > Bandwidth MGMT > Rule Setup screen allows you to edit these rule configurations.
Auto classifier rest bandwidth	Select Auto classifier rest bandwidth to automatically allocate unbudgeted or unused bandwidth to services based on the packet type.
Back	Click Back to go back to the previous wizard screen.

Table 21 Bandwidth Management Wizard: Configuration

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

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

Figure 41 Bandwidth Management Wizard: Complete

CHAPTER 5

WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

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

5.1.1 Encapsulation

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

5.1.1.1 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.

5.1.1.2 PPP over Ethernet

PPPoE (Point-to-Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

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.

5.1.1.3 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.

5.1.1.4 RFC 1483

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

5.1.2 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.

5.1.2.1 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.

5.1.2.2 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.

5.1.3 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.

5.1.4 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.

5.1.4.1 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.

5.1.4.2 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.

5.1.4.3 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.

5.1.5 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

5.1.6 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.

5.2 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 5.5 on page 90](#))
- Traffic-redirect route (see [Section 5.7 on page 99](#))
- WAN-backup route, also called dial-backup (see [Section 5.8 on page 100](#))

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

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

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

5.3 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.

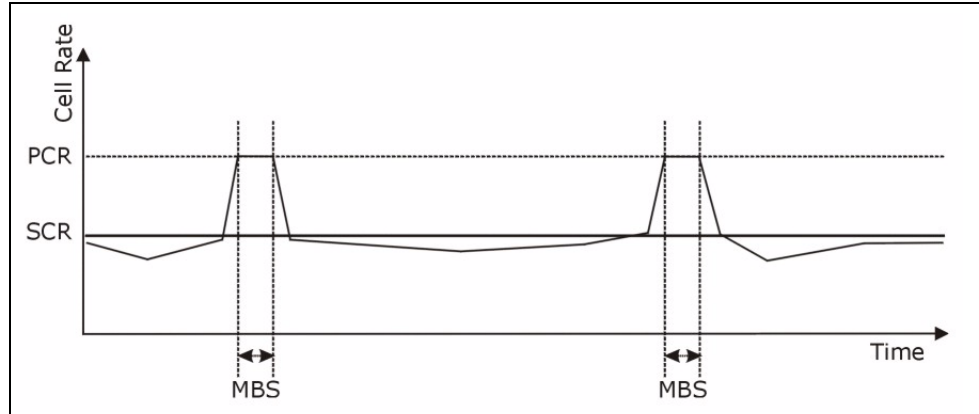
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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 42 Example of Traffic Shaping



5.3.1 ATM Traffic Classes

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

5.3.1.1 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.

5.3.1.2 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.

5.3.1.3 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.

5.4 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.

5.5 Internet Connection

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

See [Section 5.1 on page 85](#) for more information.

Figure 43 Internet Connection (PPPoE)

The following table describes the labels in this screen.

Table 22 Internet Connection

LABEL	DESCRIPTION
General	
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select Routing (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
User Name	(PPPoA and PPPoE 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 only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC .

Table 22 Internet Connection

LABEL	DESCRIPTION
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	These fields only appear if the Mode is Routing . 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.
Obtain an IP Address Automatically	(PPPoE, PPPoA, and ENET ENCAP only) Select this if you have a dynamic IP address.
Static IP Address	(PPPoE, PPPoA, and ENET ENCAP only) Select this if you do not have a dynamic IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	(ENET ENCAP only) Enter the subnet mask provided by your ISP.
Gateway IP address	(ENET ENCAP only) Enter the gateway IP address provided by your ISP.
Connection	This section only appears if the Encapsulation is PPPoE and PPPoA .
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session will not timeout.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.
Advanced Setup	Click this button to display the Advanced WAN Setup screen and edit more details of your WAN setup.

5.5.1 Configuring Advanced Internet Connection

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

Figure 44 Advanced Internet Connection

The following table describes the labels in this screen.

Table 23 Advanced Internet Connection

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the ZyXEL Device will broadcast its routing table periodically. When set to Both or In Only , it will incorporate the RIP information that it receives; when set to None , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	This field is enabled if RIP Direction is not None . The RIP Version field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (IGMP-v1) and IGMP-v2 . Select None to disable it.
ATM QoS	
ATM QoS Type	Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR-nRT (Variable Bit Rate-non Real Time) or VBR-RT (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.

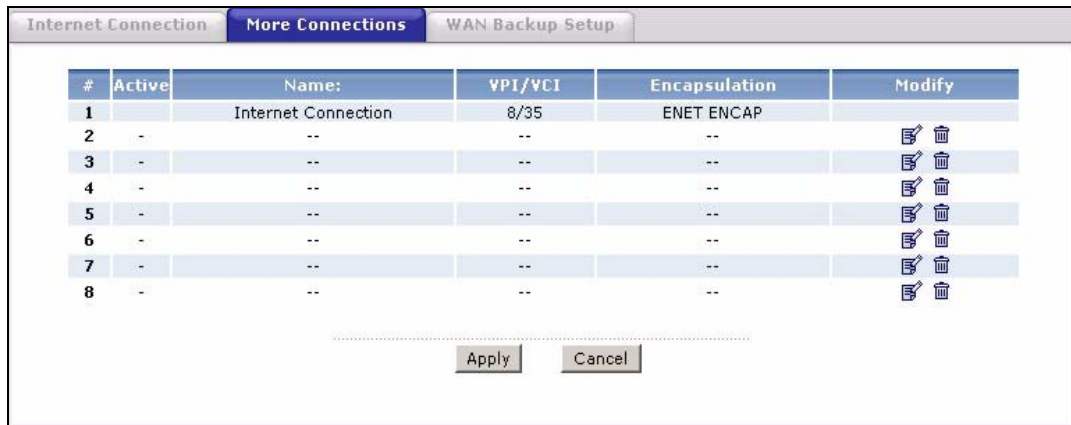
Table 23 Advanced Internet Connection

LABEL	DESCRIPTION
cell/sec	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	<p>This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode.</p> <p>Select Yes to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes.</p> <p>Select No to disable this feature. You must manually configure the ZyXEL Device for Internet access.</p>
PPPoE Passthrough (PPPoE encapsulation only)	<p>This field is available when you select PPPoE encapsulation.</p> <p>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.</p> <p>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>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.</p>
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

5.6 Configuring More Connections

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

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

Figure 45 More Connections

The following table describes the labels in this screen.

Table 24 More Connections

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

5.6.1 More Connections Edit

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

Figure 46 More Connections Edit

The following table describes the labels in this screen.

Table 25 More Connections Edit

LABEL	DESCRIPTION
Active	Select the check box to activate or clear the check box to deactivate this connection.
Name	Enter a unique, descriptive name of up to 13 ASCII characters for this connection.
Mode	Select Routing from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select Bridge , the ZyXEL Device will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices are PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.

Table 25 More Connections Edit (continued)

LABEL	DESCRIPTION
Multiplexing	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC.</p> <p>By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol.</p> <p>For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.</p>
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 Routing in the Mode field.</p> <p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.</p> <p>If you use the encapsulation type except RFC 1483, select Obtain an IP Address Automatically when you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field below.</p> <p>If you use RFC 1483, enter the IP address given by your ISP in the IP Address field.</p>
Subnet Mask	<p>Enter a subnet mask in dotted decimal notation.</p> <p>Refer to the appendices to calculate a subnet mask If you are implementing subnetting.</p>
Gateway IP address	Specify a gateway IP address (supplied by your ISP).
Connection	
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session will not timeout.
NAT	<p>SUA only is available only when you select Routing in the Mode field.</p> <p>Select SUA Only if you have one public IP address and want to use NAT. Click Edit to go to the Port Forwarding screen to edit a server mapping set.</p> <p>Otherwise, select None to disable NAT.</p>
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.
Advanced Setup	Click this button to display the More Connections Advanced screen and edit more details of your WAN setup.

5.6.2 Configuring More Connections Advanced Setup

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

Figure 47 More Connections Advanced Setup

The following table describes the labels in this screen.

Table 26 More Connections Advanced Setup

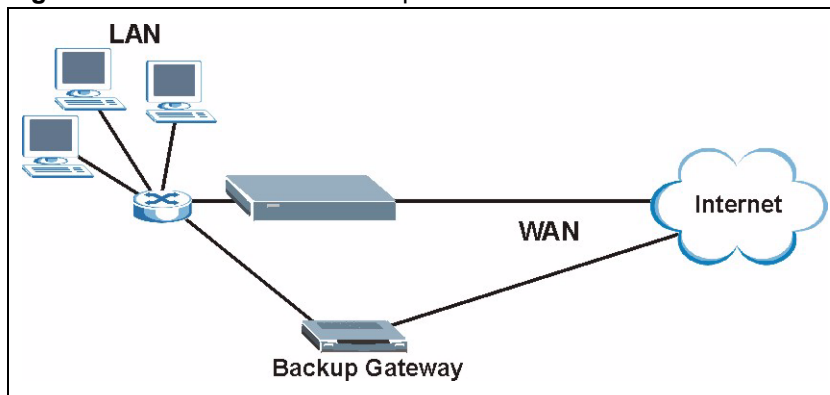
LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from None , Both , In Only and Out Only .
RIP Version	Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (IGMP-v1) and IGMP-v2 . Select None to disable it.
ATM QoS	
ATM QoS Type	Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR-nRT (Variable Bit Rate-non Real Time) or VBR-RT (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Back	Click Back to return to the previous screen.

Table 26 More Connections Advanced Setup (continued)

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

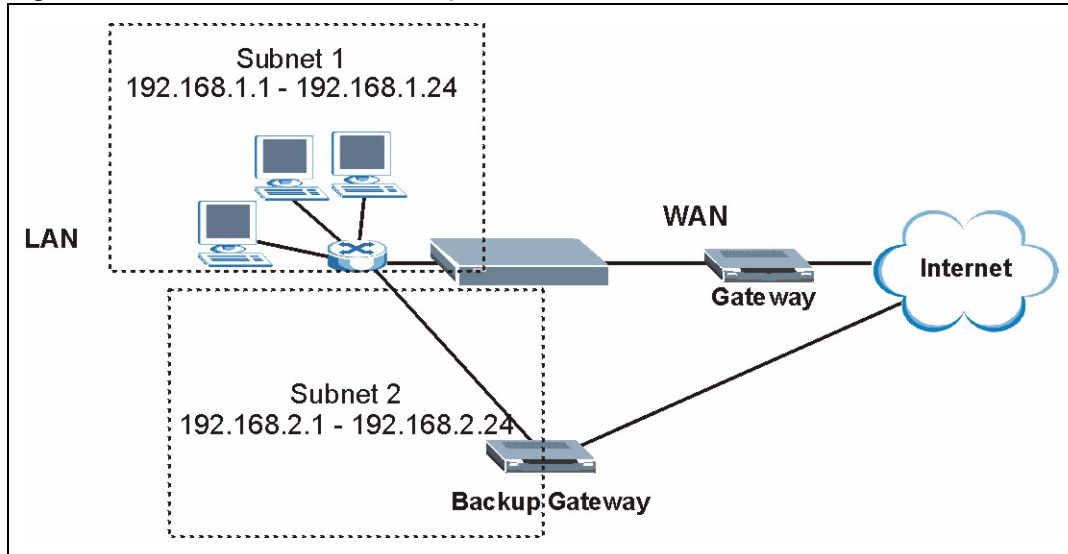
5.7 Traffic Redirect

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 48 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 49 Traffic Redirect LAN Setup



5.8 Configuring WAN Backup

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

Figure 50 WAN Backup Setup

The following table describes the labels in this screen.

Table 27 WAN Backup Setup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select DSL Link to have the ZyXEL Device check if the connection to the DSLAM is up. Select ICMP to have the ZyXEL Device periodically ping the IP addresses configured in the Check WAN IP Address fields.
Check WAN IP Address1-3	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). Note: If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the Check WAN IP Address field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.

Table 27 WAN Backup Setup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the Check WAN IP Address field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the Fail Tolerance field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.
Active Traffic Redirect	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Dial Backup	
Active Dial Backup	Select this box to activate dial up backup.
Metric	This field sets this route's priority among the three routes the ZyXEL Device uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: WAN, Traffic Redirect, Dial Backup.
Port Speed	Select the speed of the connection between the dial backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.
User Name	Enter the user name for this backup connection.
Password	Enter the password for this backup connection.
Primary Phone Number	Enter the phone number your modem should dial to create a connection.
Advanced Setup	Click this to configure advanced settings for dial backup.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

5.9 WAN Backup Advanced Screen

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

Figure 51 WAN Backup Advanced Setup

Basic	
Authentication Type	CHAP/PAP
Secondary Phone Number	
Dial Backup Port Speed	115200
AT Command Initial String	at&fs0=0
Advanced Modem Setup	Edit
TCP/IP Options	
Metric	15
<input checked="" type="checkbox"/> Enable SUA	
<input type="checkbox"/> Enable RIP	
RIP Version	RIP-2B
RIP Direction	Both
<input type="checkbox"/> Enable Multicast	
Multicast	IGMP-v2
PPP Options	
Encapsulation	Standard PPP
<input type="checkbox"/> Compression	
Connection	
<input type="radio"/> Nailed-Up Connection	
<input checked="" type="radio"/> Connect on Demand	Max Idle Timeout 100 sec
Budget	
Allocated Budget	0 min
Period	0 hr
<input style="border: none;" type="button" value=" <Back "/> <input style="border: none;" type="button" value=" Apply "/> <input style="border: none;" type="button" value=" Cancel "/>	

The following table describes the labels in this screen.

Table 28 WAN Backup Advanced Setup

LABEL	DESCRIPTION
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: CHAP/PAP - Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node. CHAP - Your ZyXEL Device accepts CHAP only. PAP - Your ZyXEL Device accept PAP only.
Secondary Phone Number	Type the secondary phone number from the ISP for this remote node. If the primary phone number is busy or does not answer, your ZyXEL Device dials the secondary phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Use the drop-down list box to select the speed of the connection between the dial backup port and the external device. Available speeds are: 9600 , 19200 , 38400 , 57600 , 115200 or 230400 bps.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

Table 28 WAN Backup Advanced Setup

LABEL	DESCRIPTION
Advanced Modem Setup	Click the Edit button to display the Advanced Modem Setup screen and edit the details of your dial backup setup.
TCP/IP Options	
Metric	<p>This field sets this route's priority among the three routes the ZyXEL Device uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority.</p> <p>If the three routes have the same metrics, the priority of the routes is as follows: WAN, Traffic Redirect, Dial Backup.</p>
Enable SUA	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network.</p> <p>SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server.</p>
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Version	<p>The RIP Version field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). Choose RIP-1, RIP-2B or RIP-2M.</p> <p>RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.</p>
RIP Direction	<p>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.</p> <p>Choose Both, In Only or Out Only.</p> <p>When set to Both or Out Only, the ZyXEL Device will broadcast its routing table periodically.</p> <p>When set to Both or In Only, the ZyXEL Device will incorporate RIP information that it receives.</p>
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast	Select IGMP-v1 or IGMP-v2 . 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.
PPP Options	
Encapsulation	Select CISCO PPP from the drop-down list box if your backup WAN device uses Cisco PPP encapsulation; otherwise select Standard PPP .
Compression	Select this check box to enable stac compression.
Connection	
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.

Table 28 WAN Backup Advanced Setup

LABEL	DESCRIPTION
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand. The default setting is 0, which means the Internet session will not timeout.
Budget	The configuration in the Budget fields has priority over your Connection settings.
Allocate Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the Period field. Set an amount that is less than the time period configured in the Period field. If you set the Allocated Budget to 0, you will not be able to use the dial backup connection.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the Allocated Budget to 10 (minutes) and the Period to 1 (hour). If you set the Period to 0, there is no budget control and the ZyXEL Device uses the Connection settings.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

5.10 Dial Backup Modem Setup

Click **Edit** in the **WAN > WAN Backup Setup > Advanced Setup** screen to configure the advanced modem settings.

Figure 52 WAN Dial Backup Modem Setup

AT Command Strings	
Dial	<input type="text" value="atd"/>
Drop	<input type="text" value="~~++++~ath"/>
Answer	<input type="text" value="ata"/>
<input type="checkbox"/> Drop DTR When Hang Up	
AT Response Strings	
CLID	<input type="text" value="NMBR ="/>
Called ID	<input type="text"/>
Speed	<input type="text" value="CONNECT"/>
Call Control	
Dial Timeout	<input type="text" value="60"/> sec
Retry Count	<input type="text" value="0"/>
Retry Interval	<input type="text" value="10"/> sec
Drop Timeout	<input type="text" value="20"/> sec
Call Back Delay	<input type="text" value="15"/> sec
<input type="button" value=" <Back"/> <input type="button" value=" Apply"/> <input type="button" value=" Cancel"/>	

The following table describes the labels in this screen.

Table 29 WAN Dial Backup Modem Setup

LABEL	DESCRIPTION
AT Command Strings	
Dial	Type the AT Command string to make a call. Example: atdt
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~++++~ath" can be used if your modem has a slow response time.
Answer	Type the AT Command string to answer a call. Example: ata
Drop DTR When Hang Up	Select this check box to have the ZyXEL Device drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.
AT Response Strings	
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyXEL Device capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication. Example: NMBR
Called ID	Type the keyword preceding the dialed number.
Speed	Type the keyword preceding the connection speed. Example: CONNECT
Call Control	
Dial Timeout	Type a number of seconds for the ZyXEL Device to try to set up an outgoing call before timing out (stopping). Example: 60
Retry Count	Type a number of times for the ZyXEL Device to retry a busy or no-answer phone number before blacklisting the number. Example: 0

Table 29 WAN Dial Backup Modem Setup

LABEL	DESCRIPTION
Retry Interval	Type a number of seconds for the ZyXEL Device to wait before trying another call after a call has failed. This applies before a phone number is blacklisted. Example: 10
Drop Timeout	Type the number of seconds for the ZyXEL Device to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. Example: 20
Call Back Delay	Type a number of seconds for the ZyXEL Device to wait between dropping a callback request call and dialing the corresponding callback call. Example: 15
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 6

LAN Setup

This chapter describes how to configure LAN settings.

6.1 LAN Overview

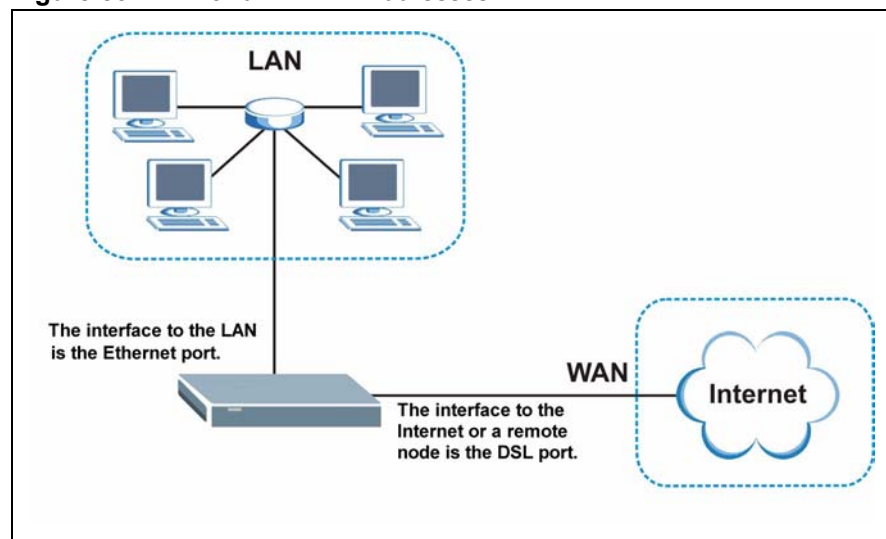
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 6.3 on page 115](#) to configure the LAN screens.

6.1.1 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 53 LAN and WAN IP Addresses



6.1.2 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.

6.1.2.1 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.

6.1.3 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 the **Primary** and **Secondary DNS Server** fields in the **DHCP Setup** screen are not specified, for instance, left as **0.0.0.0**, the ZyXEL Device tells the DHCP clients that it 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 the 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.

6.1.4 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 **Primary** and **Secondary DNS Server** fields are left as **0.0.0.0** in the **DHCP Setup** screen.

6.2 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.

6.2.1 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.

6.2.1.1 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*.

6.2.2 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.

6.2.3 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.

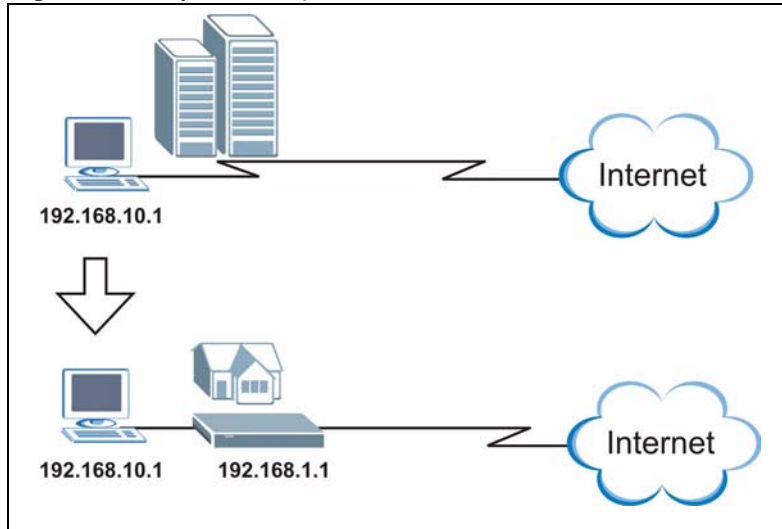
The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on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

6.2.4 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 54 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.

6.2.4.1 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.

6.3 Configuring LAN IP

Click **LAN** to open the **IP** screen. See [Section 6.1 on page 109](#) for background information.

Figure 55 LAN IP

The following table describes the fields in this screen.

Table 30 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 Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.
Advanced Setup	Click this button to display the Advanced LAN Setup screen and edit more details of your LAN setup.

6.3.1 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 56 Advanced LAN Setup

The following table describes the labels in this screen.

Table 31 Advanced LAN Setup

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

6.4 DHCP Setup

Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

Figure 57 DHCP Setup

The following table describes the labels in this screen.

Table 32 DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	<p>If set to Server, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to None, the DHCP server will be disabled.</p> <p>If set to Relay, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>
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	If Relay is selected in the DHCP field above then enter the IP address of the actual remote DHCP server here.
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 32 DHCP Setup

LABEL	DESCRIPTION
Primary DNS Server	This field is not available when you set DHCP to Relay .
Secondary 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. If the fields are left as 0.0.0.0, the ZyXEL Device acts as a DNS proxy and forwards the DHCP client's DNS query to the real DNS server learned through IPCP and relays the response back to the computer.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to begin configuring this screen afresh.

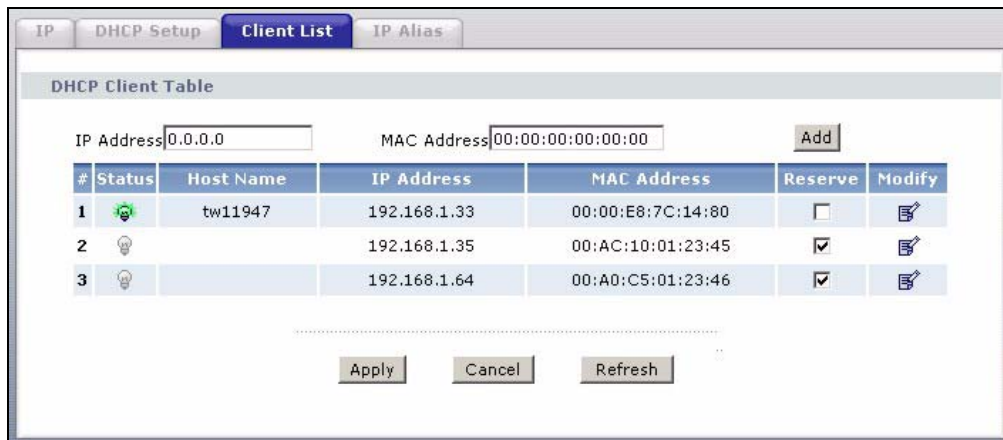
6.5 LAN Client List

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.

To change your ZyXEL Device's static DHCP settings, click **Network > LAN > Client List**. The screen appears as shown.

Figure 58 LAN Client List



The following table describes the labels in this screen.

Table 33 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 specified below. The IP address should be within the range of IP addresses you specified in the DHCP Setup for the DHCP client.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click Add to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 32 entries in this table.
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.
Refresh	Click Refresh to reload the DHCP table.

6.6 LAN IP Alias

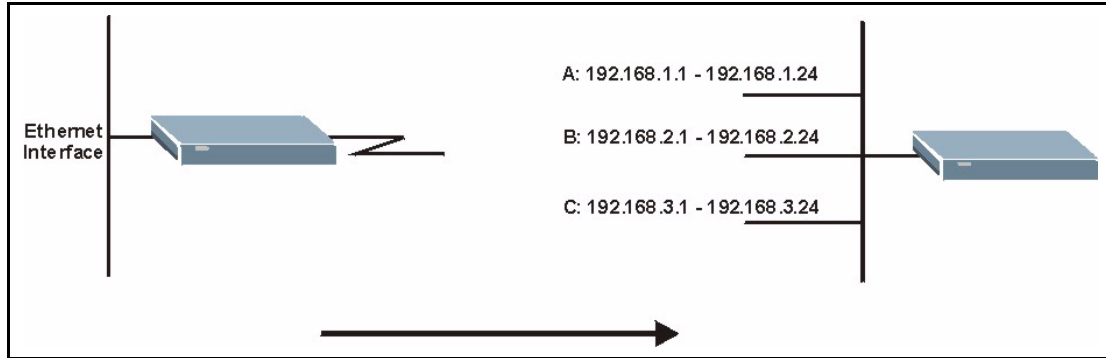
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

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.

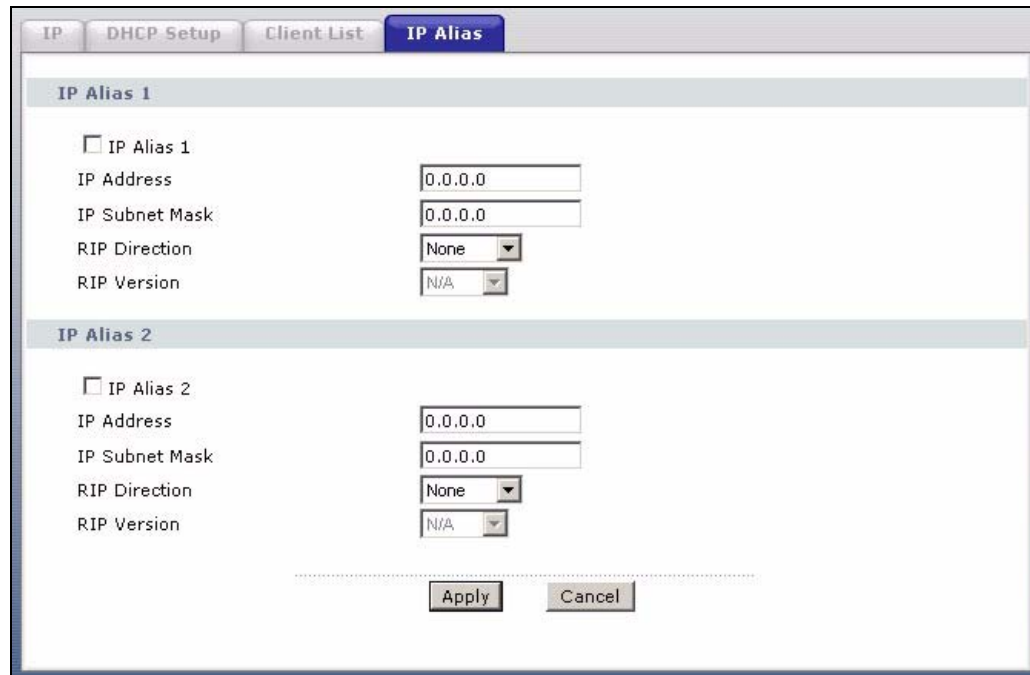
The following figure shows a LAN divided into subnets A, B, and C.

Figure 59 Physical Network & Partitioned Logical Networks



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

Figure 60 LAN IP Alias



The following table describes the labels in this screen.

Table 34 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 34 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 RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the ZyXEL Device will broadcast its routing table periodically. When set to Both or In Only , it will incorporate the RIP information that it receives; when set to None , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The RIP Version field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 7

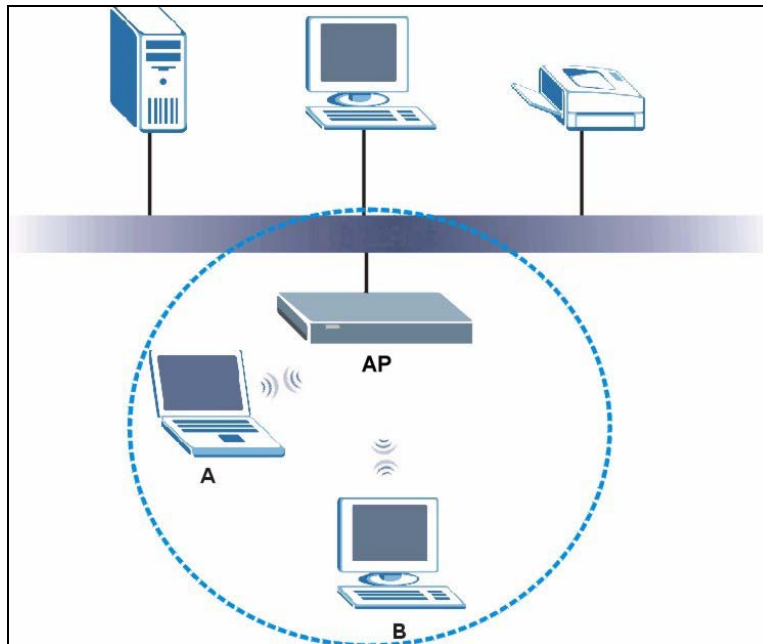
Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. This chapter applies to the P-662HW-D models only.

7.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 61 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.

7.2 Wireless Security Overview

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

7.2.1 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.

7.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each 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.

7.2.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every 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, there are two typical places to store the user names and passwords for each user.

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

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

Unauthorized 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.

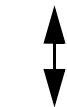
Local user databases also have an additional limitation that is explained in the next section.

7.2.4 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 7.2.3 on page 124](#) for information about this.)

Table 35 Types of Encryption for Each Type of Authentication

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

For example, if the wireless network has a RADIUS server, you can choose **IEEE 802.1x**, **IEEE 802.1x + Static WEP**, **IEEE 802.1x + Dynamic WEP**, **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device. The ZyXEL Device does not have a local user database, 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. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

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.

7.2.5 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 7.6 on page 135](#) for more details.

7.3 Wireless Performance Overview

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

7.3.1 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.

7.4 Additional Wireless Terms

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

Table 36 Additional Wireless Terms

TERM	DESCRIPTION
Intra-BSS Traffic	This describes direct communication (not through the ZyXEL Device) between two wireless devices within a wireless network. You might disable this kind of communication to enhance security within your wireless network.
RTS/CTS Threshold	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. 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. 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.
Preamble	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.
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.

7.5 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 **General** screen.

Figure 62 Wireless LAN: General

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

Table 37 Wireless LAN: General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate wireless LAN. Note: You can also activate the wireless LAN by pressing the RESET button for 1 second.
Network Name(SSID)	(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. 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.
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	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. Select a channel from the drop-down list box.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.
Advanced Setup	Click Advanced Setup to display the Wireless Advanced Setup screen and edit more details of your WLAN setup.

See the rest of this chapter for information on the other labels in this screen.

7.5.1 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 63 Wireless: No Security

The screenshot shows the 'Wireless Setup' configuration page. It has tabs for 'General', 'DTIST', 'MAC Filter', and 'QoS'. The 'General' tab is selected. Under 'Wireless Setup', there is a checked box for 'Active Wireless LAN'. The 'Network Name(SSID)' is set to 'ZyXEL'. There is an unchecked box for 'Hide SSID'. The 'Channel Selection' is set to 'Channel-06 2437MHz'. Under the 'Security' section, the 'Security Mode' is set to 'No Security'. At the bottom, there are three buttons: 'Apply', 'Cancel', and 'Advanced Setup'.

The following table describes the labels in this screen.

Table 38 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose No Security from the drop-down list box.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.
Advanced Setup	Click Advanced Setup to display the Wireless Advanced Setup screen and edit more details of your WLAN setup.

7.5.2 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 64 Wireless: Static WEP Encryption

The screenshot shows the 'Wireless Setup' and 'Security' sections of a ZyXEL router's configuration page. In the 'Wireless Setup' section, 'Active Wireless LAN' is checked, the Network Name (SSID) is 'ZyXEL', 'Hide SSID' is unchecked, and the Channel Selection is 'Channel-06 2437MHz'. In the 'Security' section, the Security Mode is set to 'Static WEP'. The Passphrase field contains 'fvoluyvdlc' and has a 'Generate' button next to it. The WEP Key field contains '292325f9e4'. Below the fields is a 'Note' section with instructions on WEP key lengths and character sets. At the bottom are 'Apply', 'Cancel', and 'Advanced Setup' buttons.

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

Table 39 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose Static WEP from the drop-down list box.
Passphrase	Enter a Passphrase (up to 32 printable characters) and click Generate . The ZyXEL Device automatically generates a WEP key.
WEP Key	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless 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.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.
Advanced Setup	Click Advanced Setup to display the Wireless Advanced Setup screen and edit more details of your WLAN setup.

7.5.3 WPA(2)-PSK

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

Figure 65 Wireless: WPA(2)-PSK

The screenshot shows the 'Wireless Setup' and 'Security' sections of a ZyXEL configuration page. The 'Wireless Setup' section includes a checked 'Active Wireless LAN' box, a 'Network Name(SSID)' field containing 'ZyXEL', an unchecked 'Hide SSID' box, and a 'Channel Selection' dropdown menu set to 'Channel-06 2437MHz'. The 'Security' section features a 'Security Mode' dropdown menu set to 'WPA2-PSK', an unchecked 'WPA Compatible' box, an empty 'Pre-Shared Key' field, and three timer fields: 'ReAuthentication Timer' (1800), 'Idle Timeout' (3600), and 'Group Key Update Timer' (1800), all with '(In Seconds)' labels. At the bottom are 'Apply', 'Cancel', and 'Advanced Setup' buttons.

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

Table 40 Wireless: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose WPA-PSK or WPA2-PSK from the drop-down list box.
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. 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). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (In Seconds)	The ZyXEL Device automatically disconnects a wireless 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).

Table 40 Wireless: WPA(2)-PSK

LABEL	DESCRIPTION
Group Key Update Timer (In Seconds)	The Group Key Update Timer is the rate at which the AP (if using WPA(2)-PSK key management) or RADIUS server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA(2)-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.
Advanced Setup	Click Advanced Setup to display the Wireless Advanced Setup screen and edit more details of your WLAN setup.

7.5.4 WPA(2) Authentication Screen

In order to configure and enable WPA(2) Authentication; click the **Wireless LAN** link under **Network** to display the **Wireless** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 66 Wireless: WPA(2)

The screenshot shows the 'Wireless Setup' and 'Security' configuration pages. The 'Wireless Setup' section includes a checked 'Active Wireless LAN' checkbox, a text field for 'Network Name(SSID)' containing 'ZyXEL', an unchecked 'Hide SSID' checkbox, and a dropdown menu for 'Channel Selection' set to 'Channel-06 2437MHz'. The 'Security' section features a dropdown for 'Security Mode' set to 'WPA2', an unchecked 'WPA Compatible' checkbox, and three text input fields for timers: 'ReAuthentication Timer' (1800), 'Idle Timeout' (3600), and 'Group Key Update Timer' (1800), each with '(In Seconds)' to its right. Below these are two sets of fields for servers: 'Authentication Server' with IP Address (0.0.0.0), Port Number (1812), and Shared Secret; and 'Accounting Server (optional)' with IP Address (0.0.0.0), Port Number (1813), and Shared Secret. At the bottom of the form are three buttons: 'Apply', 'Cancel', and 'Advanced Setup'.

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

Table 41 Wireless: WPA(2)

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
ReAuthentication Timer (In Seconds)	Specify how often wireless 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). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (In Seconds)	The ZyXEL Device automatically disconnects a wireless 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 (In Seconds)	The Group Key Update Timer is the rate at which the AP (if using WPA(2)-PSK key management) or RADIUS server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA(2)-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server (optional)	
Active	Select Yes from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is 1813 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click Apply to save your changes back to the ZyXEL Device.

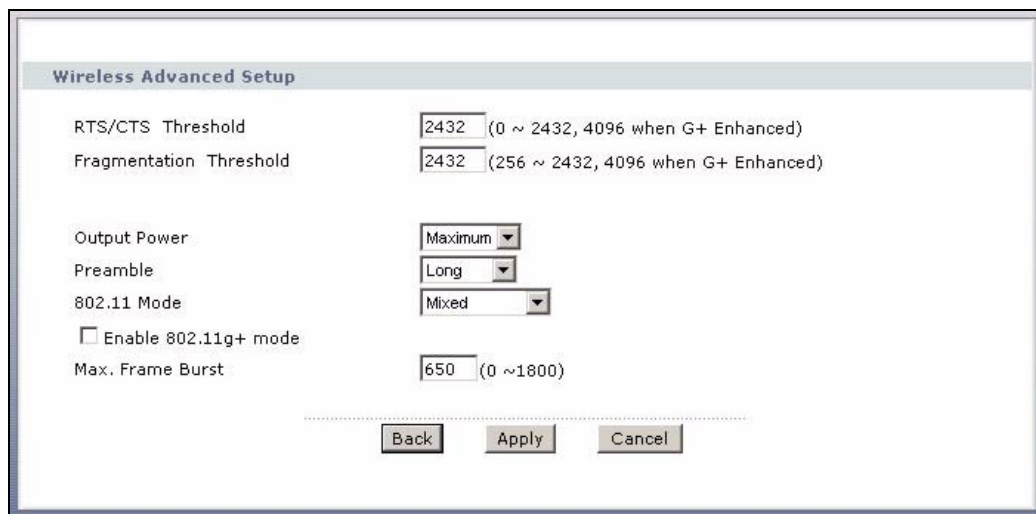
Table 41 Wireless: WPA(2)

LABEL	DESCRIPTION
Cancel	Click Cancel to reload the previous configuration for this screen.
Advanced Setup	Click Advanced Setup to display the Wireless Advanced Setup screen and edit more details of your WLAN setup.

7.5.5 Wireless LAN Advanced Setup

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

Figure 67 Advanced



The following table describes the labels in this screen.

Table 42 Wireless LAN: Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Enter a value between 0 and 2432. If you select the Enable 802.11g+ mode checkbox, this field is grayed out and the ZyXEL Device uses 4096 automatically.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. If you select the Enable 802.11g+ mode checkbox, this field is grayed out and the ZyXEL Device uses 4096 automatically.
Output Power	Set the output power of the ZyXEL Device in this field. This control changes the strength of the ZyXEL Device's antenna gain or transmission power. Antenna gain is the increase in coverage. Higher antenna gain improves the range of the signal for better communications. If there is a high density of APs within an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. The options are Maximum , Middle and Minimum .
Preamble	Select a preamble type from the drop-down list menu. Choices are Long , Short or Dynamic . The default setting is Long . See the section on preamble for more information.

Table 42 Wireless LAN: Advanced

LABEL	DESCRIPTION
802.11 Mode	Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Enable 802.11g+ mode	Select Enable 802.11g+ mode checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the ZyXEL Device at higher transmission speeds. This permits the ZyXEL Device to transmit at a higher speed than the 802.11g Only mode.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in micro-seconds, that the ZyXEL Device transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.

7.6 OTIST

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

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

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

7.6.1 Enabling OTIST

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

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

7.6.1.1 AP

Click the **Wireless LAN** link under **Network** and then the **OTIST** tab. The following screen displays.

Figure 68 OTIST



The following table describes the labels in this screen.

Table 43 OTIST

LABEL	DESCRIPTION
Setup Key	Type an OTIST Setup Key of exactly eight ASCII characters in length. The default OTIST setup key is "01234567". Note: If you change the OTIST setup key here, you must also make the same change on the wireless client(s).

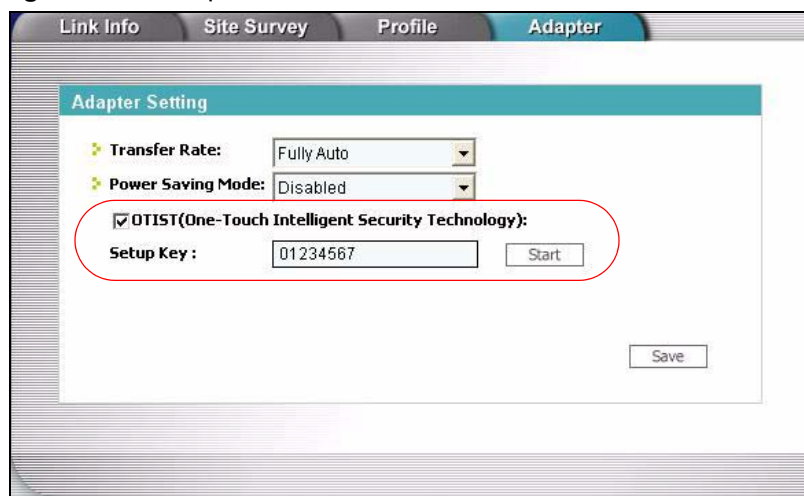
Table 43 OTIST

LABEL	DESCRIPTION
Yes!	<p>If you want to configure your own WPA-PSK and have OTIST use that WPA-PSK, you must:</p> <ul style="list-style-type: none"> • Configure a WPA-PSK in the Wireless > General screen. • Clear the Yes! checkbox in the OTIST screen and click Start. <p>Note: If you already have a WPA-PSK configured in the Wireless screen, and you run OTIST with Yes! selected, OTIST will not replace the WPA-PSK. Clear the checkbox in the OTIST screen.</p> <p>If you want OTIST to automatically generate a WPA-PSK, you must:</p> <ul style="list-style-type: none"> • Change your security to No Security in the Wireless > General screen. • Select the Yes! checkbox in the OTIST screen and click Start. • The wireless screen displays an auto generated WPA-PSK and is now in WPA-PSK security mode. <p>The WPA-PSK security settings are assigned to the wireless client when you start OTIST.</p>
Start	<p>Click Start to encrypt the wireless security data using the setup key and have the ZyXEL Device set the wireless station to use the same wireless settings as the ZyXEL Device. You must also activate and start OTIST on the wireless station at the same time.</p> <p>The process takes three minutes to complete.</p> <p>Note: You can also start OTIST by pressing the RESET button for 3 seconds.</p>

7.6.1.2 Wireless Client

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

Figure 69 Example Wireless Client OTIST Screen

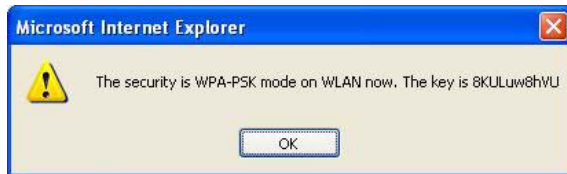


7.6.2 Starting OTIST

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

- 1 In the AP, a web configurator screen pops up showing you the security settings to transfer. After reviewing the settings, click **OK**.

Figure 70 Security Key

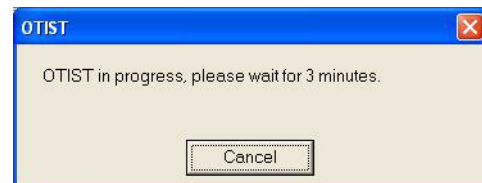


- 2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.

Figure 71 OTIST in Progress (AP)



Figure 72 OTIST in Progress (Client)



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

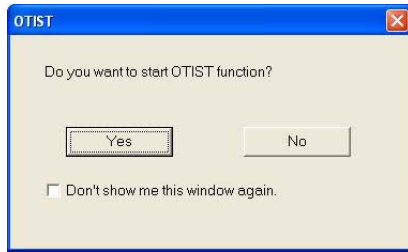
Figure 73 No AP with OTIST Found



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

7.6.3 Notes on OTIST

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

Figure 74 Start OTIST?

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

7.7 MAC Filter

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to up to 32 devices (**Allow**) or exclude up to 32 devices from accessing the ZyXEL Device (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

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

Figure 75 MAC Address Filter

The following table describes the labels in this menu.

Table 44 MAC Address Filter

LABEL	DESCRIPTION
Active MAC Filter	Select the check box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC Address table. Select Deny to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device Select Allow to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless 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.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to reload the previous configuration for this screen.

7.8 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks for multimedia applications.

WMM allows you to prioritize wireless traffic according to the delivery requirements of the individual and applications.

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

7.8.1 WMM QoS Example

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

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

7.8.2 WMM QoS Priorities

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

Table 45 WMM QoS Priorities

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

7.8.3 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 46 Commonly Used Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.

Table 46 Commonly Used Services

SERVICE	DESCRIPTION
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
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.

7.9 QoS Screen

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

7.9.1 ToS (Type of Service) and WMM QoS

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

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

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

Figure 76 Wireless LAN: QoS

#	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	-	

The following table describes the fields in this screen.

Table 47 Wireless LAN: QoS

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

Table 47 Wireless LAN: QoS

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

7.9.2 Application Priority Configuration

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

Figure 77 Application Priority Configuration

The following table describes the fields in this screen.

Table 48 Application Priority Configuration

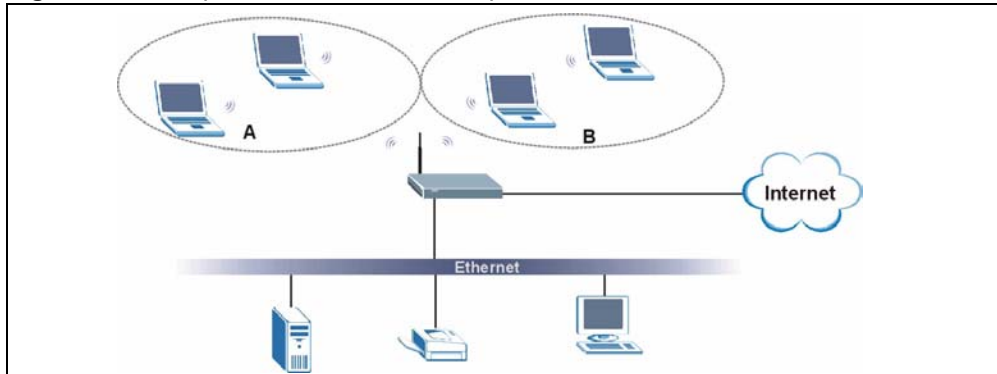
LABEL	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.

Table 48 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"> • FTP File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21. • E-Mail Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80 • WWW The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser. • User-Defined User-defined services are user specific services configured using known ports and applications.
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. See Table 46 on page 143 for information on port numbers.
Priority	Select a priority from the drop-down list box. See Table 45 on page 141 for more information on specific priorities.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previous screen without saving your changes.

7.10 Multiple SSID (P-662HW-D Models only)

The ZyXEL Device supports multiple SSID which allows you to configure a second wireless network with its own security parameters. This means that you can allow two different user groups to be connected to the same access point. Each user group can have different security options and access to different resources on your network. For example, in an office, one permanent user group (**A**) can have access to the entire network and a second user group (**B**) can connect to the access point and use the wireless connection to only browse the Internet.

Figure 78 Multiple SSID Network Example

In this section the second wireless network is referred to as the “guest wireless network” and user’s connecting to this network are referred to as “guests”.

Multiple SSID is only configurable via commands. The next sections describe multiple SSID commands and show a configuration example. See [Appendix H on page 419](#) for information on the command structure and how to access the CLI (Command Line Interface) on the ZyXEL Device.

7.10.1 Multiple SSID Commands

Use the `wlan mssid` commands to configure multiple SSID on the ZyXEL Device. The commands must be entered in the following syntax:

```
wlan mssid guestssid <ssid>
wlan mssid mode [0:disable guestssid 1:enable guestssid] [0:disable
-> intranet blocking 1:enable intranet blocking]
wlan mssid setprivacy type <0:NO 1:WEP64 2:WEP128 3:WEP256>
wlan mssid setprivacy key <1-4> <Key String>
wlan mssid setprivacy defaultkey <1-4>
wlan mssid guest_autoOff < <1:on, 0:off> <Timeout (minutes), 0 for
-> default>
wlan mssid show
```

The following table gives a description of multiple SSID commands.

Table 49 Multiple SSID Commands

Command	Description
guestssid <SSID>	Use this command to specify the SSID of the guest wireless network. This is the SSID guests have to configure on their wireless clients to connect to your wireless network. Type a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
mode [0:disable guestssid 1:enable guestssid] [0:disable intranet blocking 1:enable intranet blocking]	This command performs two functions and is followed by two parameters. The first parameter specifies whether you want to enable or disable your guest wireless network. Type 0 to disable the guest wireless network or type 1 to enable the guest wireless network. The second parameter specifies whether you want to block guests in the guest wireless network from accessing resources on your LAN. Type 0 to allow guests to access resources on your LAN or type 1 to block guests from accessing resources on your LAN and only allow access to the Internet via the ZyXEL Device.
setprivacy type <0:NO 1:WEP64 2:WEP128 3:WEP256>	This command specifies the security mode for the guest wireless network. Type one of the following: 0 to disable security on the guest wireless network, 1 to enable 64-bit WEP key encryption, 2 to enable 128-bit WEP key encryption, 3 256-bit WEP key encryption.
setprivacy wepkey <1-4> <Key String>	This command allows you to create up to four WEP keys. Enter 1 , 2 , 3 or 4 to specify which WEP key you are creating followed by 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.
setprivacy defaultkey <1-4>	This command specifies which WEP key guests have to configure on their wireless clients to access the guest wireless network.
guest_autoOff < <1:on, 0:off> <Timeout (minutes), 0 for default>	This command enables or disables an automatic timeout feature of the guest wireless network. If you enable this feature the guest wireless network becomes disabled after the specified amount of time. You need to enter two parameters. Type 0 to disable the automatic timeout feature or type 1 to enable it, for the next value enter the number of minutes that the guest wireless network stays active. Enter a number from 0 to 30000. Entering 0 resets the value to the default (60 minutes). Note: This command is hidden. It doesn't show up when you type the wlan mssid command.
show	This command allows you to review your guest wireless network settings.

7.10.2 Multiple SSID Example

This example shows how to configure a guest wireless network with the following parameters.

Table 50 Multiple SSID Example Configuration

PARAMETER	VALUE
SSID	guestnetwork
Security	64-bit WEP key encryption.
WEP key	abcde
Other	Intranet blocking is enabled, so that guests only have access to the Internet and cannot access the local network.

In the following script example all typed commands and parameters have been bolded.

```

ras> wlan mssid guestssid guestnetwork
Note: the wireless connection will be disconnected temporarily!!!
ras> wlan mssid mode 1 1
Note: the wireless connection will be disconnected temporarily!!!
Enable GuestSSID
GuestSSID with Intranet Blocking
TFTP Client Start
ras> wlan mssid setprivacy type 1
Privacy Setting is WEP64
Note: the wireless connection will be disconnected temporarily!!!
TFTP Client Start
ras> wlan mssid setprivacy wepkey 1 abcde
Note: the wireless connection will be disconnected temporarily!!!
TFTP Client Start
ras> wlan mssid show
Multiple SSID Settings :

==Major SSID Settings ==
Major SSID = "Wireless"
Major SSID privacy setting is WPA

==Guest SSID Settings ==
Guest SSID = Enable
Guest SSID = "guestnetwork"
Guest SSID privacy setting is WEP 64
WEP default key ID = 1
WEP key 1 = abcde
WEP key 2 =
WEP key 3 =
WEP key 4 =
Intranet Blocking = 1
Guest SSID AutoOff = Disable
Guest SSID AutoOff Timeout = 0 (minutes)
ras>

```

CHAPTER 8

DMZ

This chapter describes how to configure the ZyXEL Device's DMZ.

8.1 Introduction

The DeMilitarized Zone (DMZ) auto-negotiating 10/100 Mbps Ethernet port provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

It is highly recommended that you connect all of your public servers to the DMZ port. If you have more than one public server, connect a hub to the DMZ port.

It is also highly recommended that you keep all sensitive information off of the public servers connected to the DMZ port. Store sensitive information on LAN computers.

8.2 Configuring DMZ

You can assign public or private IP addresses to computers connected to the DMZ port.

With public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See the appendix for information on IP subnetting.

From the main menu, click **Network > DMZ**. The screen appears as shown next.

Figure 79 DMZ

DMZ TCP/IP	
IP Address	192.168.2.1
IP Subnet Mask	255.255.255.0
RIP Direction	None
RIP Version	Non Applicable
Multicast	None
Windows Networking (NetBIOS over TCP/IP)	
<input checked="" type="checkbox"/>	Allow between DMZ and LAN (You also need to create a firewall rule!)
<input checked="" type="checkbox"/>	Allow between DMZ and WAN
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 51 DMZ

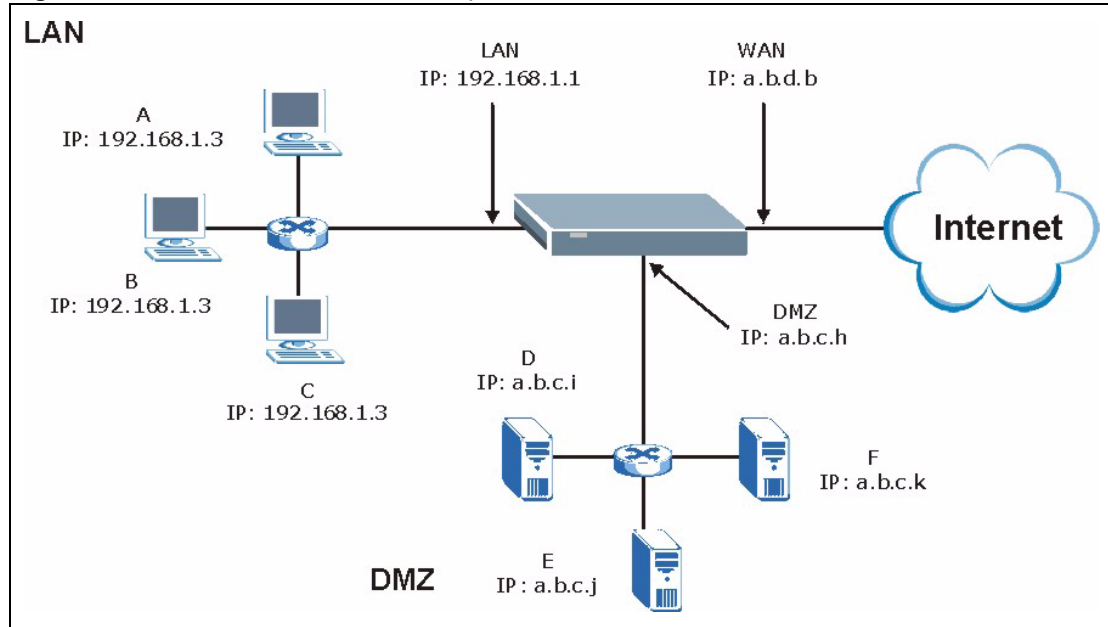
LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your ZyXEL Device's DMZ port in dotted decimal notation. Make sure the IP address is on a separate subnet from the LAN port.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the ZyXEL Device will broadcast its routing table periodically. When set to Both or In Only , it will incorporate the RIP information that it receives; when set to None , it will not send any RIP packets and will ignore any RIP packets received. Both is the default.
RIP Version	The RIP Version field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (IGMP-v1) and IGMP-v2 . Select None to disable it.
Windows Networking (NetBIOS over TCP/IP)	

Table 51 DMZ (continued)

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

8.3 DMZ Public IP Address Example

The following figure shows a simple network setup with public IP addresses on the WAN and DMZ and private IP addresses on the LAN. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet. The DMZ port and connected servers (D through F) use public IP addresses that are in another subnet. The public IP addresses of the DMZ and WAN ports are in separate subnets.

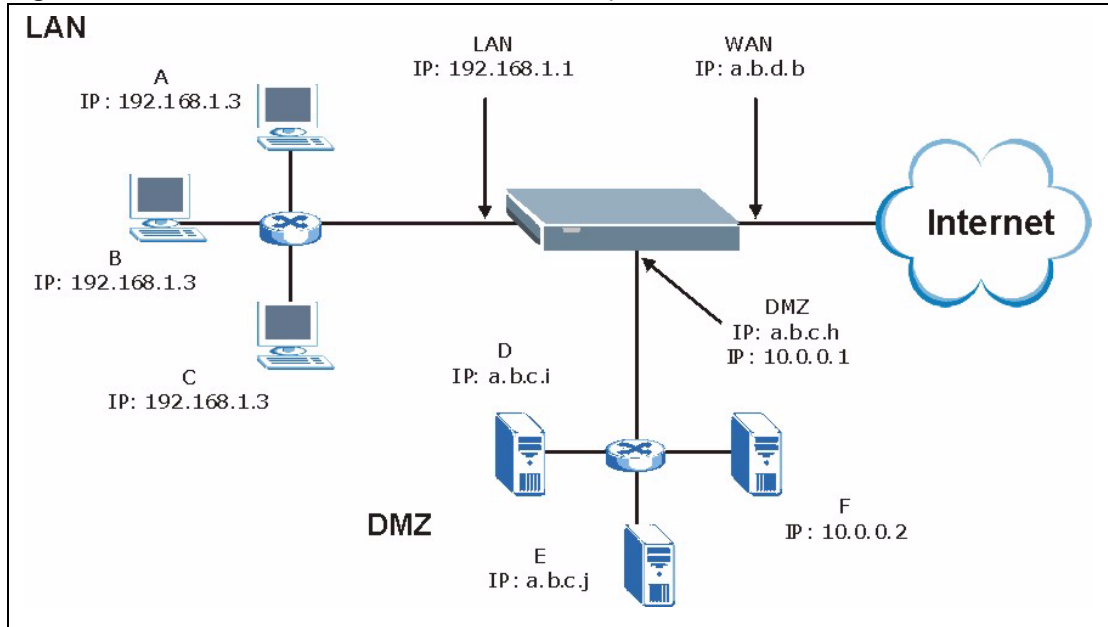
Figure 80 DMZ Public Address Example

8.4 DMZ Private and Public IP Address Example

The following figure shows a network setup with both private and public IP addresses on the DMZ. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet. The DMZ port and server F use private IP addresses that are in one subnet. The private IP addresses of the LAN and DMZ are on separate subnets. The DMZ port and connected servers (D and E) use public IP addresses that are in one subnet. The public IP addresses of the DMZ and WAN are on separate subnets.

Configure both DMZ and DMZ IP alias to use this kind of network setup. You also need to configure NAT for the private DMZ IP addresses.

Figure 81 DMZ Private and Public Address Example



CHAPTER 9

Network Address Translation (NAT) Screens

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

9.1 NAT Overview

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

9.1.1 NAT Definitions

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

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

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

Table 52 NAT Definitions

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

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

9.1.2 What NAT Does

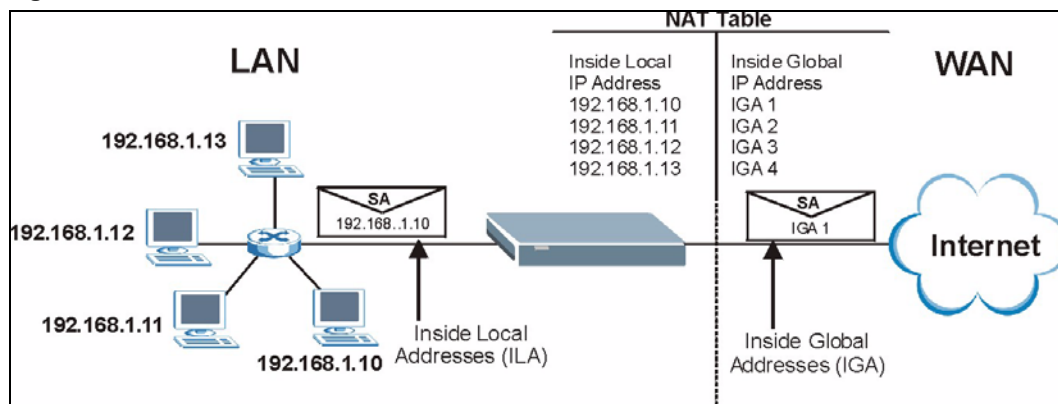
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 53 on page 160](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

9.1.3 How NAT Works

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

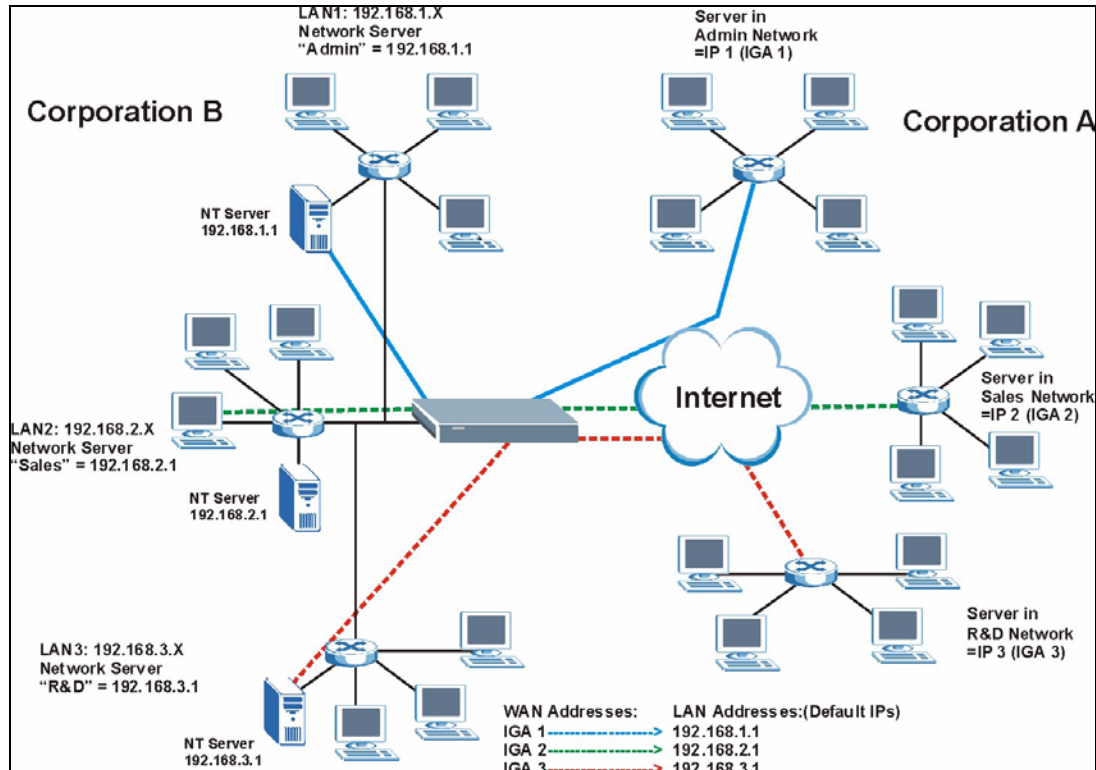
Figure 82 How NAT Works



9.1.4 NAT Application

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

Figure 83 NAT Application With IP Alias



9.1.5 NAT Mapping Types

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

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

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

The following table summarizes these types.

Table 53 NAT Mapping Types

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

9.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 53 on page 160](#).

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

9.3 NAT General Setup

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

Figure 84 NAT General

The following table describes the labels in this screen.

Table 54 NAT General

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

9.4 Port Forwarding

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

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

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

9.4.1 Default Server IP Address

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

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

9.4.2 Port Forwarding: Services and Port Numbers

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

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

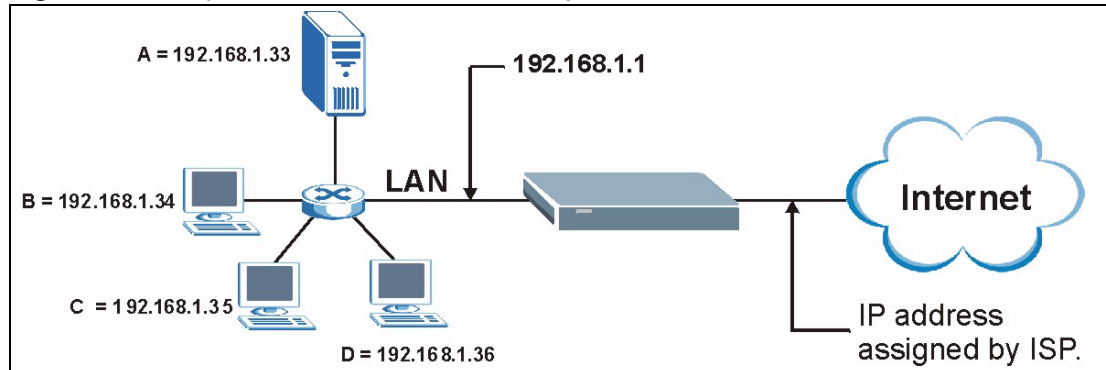
Table 55 Services and Port Numbers

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

9.4.3 Configuring Servers Behind Port Forwarding (Example)

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

Figure 85 Multiple Servers Behind NAT Example



9.5 Configuring Port Forwarding

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

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

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

See [Table 55 on page 162](#) for port numbers commonly used for particular services.

Figure 86 NAT Port Forwarding

The screenshot shows the NAT Port Forwarding configuration screen. The 'Port Forwarding' tab is selected. Under 'Default Server Setup', the 'Default Server' is set to 0.0.0.0. Under 'Port Forwarding', the 'Service Name' is set to WWW and the 'Server IP Address' is set to 0.0.0.0. A table lists the port forwarding rules, with one rule for WWW on port 80, pointing to server IP 172.23.15.23.

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

The following table describes the fields in this screen.

Table 56 NAT Port Forwarding

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

9.5.1 Port Forwarding Rule Edit

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

Figure 87 Port Forwarding Rule Setup

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

- An "Active" checkbox that is checked.
- A "Service Name" text input field containing the text "WWW".
- A "Start Port" text input field containing the number "80".
- An "End Port" text input field containing the number "80".
- A "Server IP Address" text input field containing the IP address "10.10.1.2".
- At the bottom of the form, there are three buttons: "Back", "Apply", and "Cancel".

The following table describes the fields in this screen.

Table 57 Port Forwarding Rule Setup

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

9.6 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 88 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 58 Address Mapping Rules

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

9.6.1 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 89 Edit Address Mapping Rule

The screenshot shows a web-based configuration interface titled "Edit Address Mapping Rule 1". It 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 currently set to "N/A", with a blue link labeled "Edit Details" next to it.

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

The following table describes the fields in this screen.

Table 59 Edit Address Mapping Rule

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <ul style="list-style-type: none"> • One-to-One: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. • Many-to-One: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. • Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. • Many-to-Many No Overload: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. • Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are N/A for Server 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 Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-One and Server mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Server Mapping Set	Only available when Type is set to Server . Select a number from the drop-down menu to choose a server mapping set.

Table 59 Edit Address Mapping Rule (continued)

LABEL	DESCRIPTION
Edit Details	Click this link to go to the Port Forwarding screen to edit a server mapping set that you have selected in the Server Mapping Set field.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 10

Firewalls

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

10.1 Firewall Overview

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

Refer to [Section 11.5 on page 184](#) to configure default firewall settings.

Refer to [Section 11.6 on page 185](#) to view firewall rules.

Refer to [Section 11.6.1 on page 187](#) to configure firewall rules.

Refer to [Section 11.6.2 on page 190](#) to configure a custom service.

Refer to [Section 11.10.3 on page 200](#) to configure firewall thresholds.

10.2 Types of Firewalls

There are three main types of firewalls:

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

10.2.1 Packet Filtering Firewalls

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

10.2.2 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.

10.2.3 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 10.5 on page 175](#) for more information on stateful inspection.

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

10.3 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.

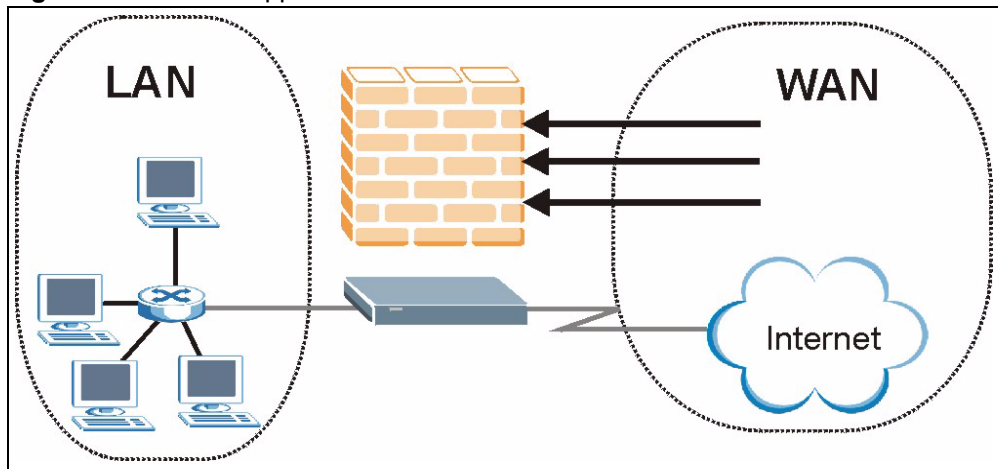
The ZyXEL Device has one DSL/ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

- 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.

10.3.1 Denial of Service Attacks

Figure 90 Firewall Application



10.4 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.

10.4.1 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:

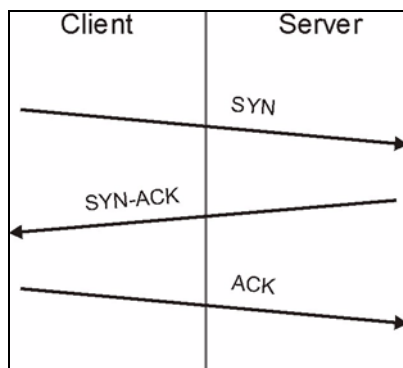
Table 60 Common IP Ports

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

10.4.2 Types of DoS Attacks

There are four types of DoS attacks:

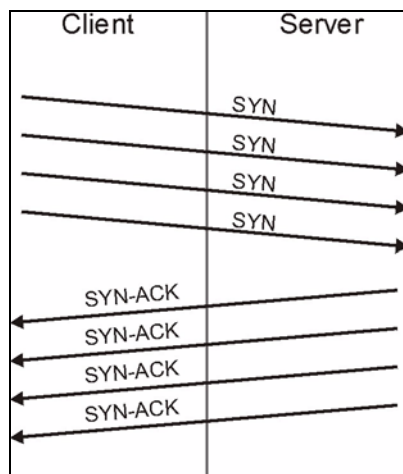
- 1 Those that exploit bugs in a TCP/IP implementation.
- 2 Those that exploit weaknesses in the TCP/IP specification.
- 3 Brute-force attacks that flood a network with useless data.
- 4 IP Spoofing.
- 5 **"Ping of Death"** and **"Teardrop"** attacks exploit bugs in the TCP/IP implementations of various 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 91 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.

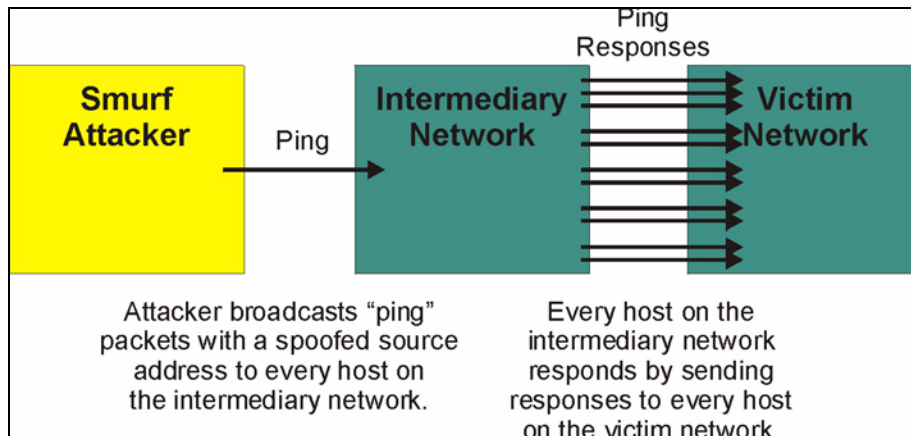
- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs 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 92 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 93 Smurf Attack



10.4.2.1 ICMP Vulnerability

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

Table 61 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

10.4.2.2 Illegal Commands (NetBIOS and SMTP)

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

Table 62 Legal NetBIOS Commands

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

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

Table 63 Legal SMTP Commands

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

10.4.2.3 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.

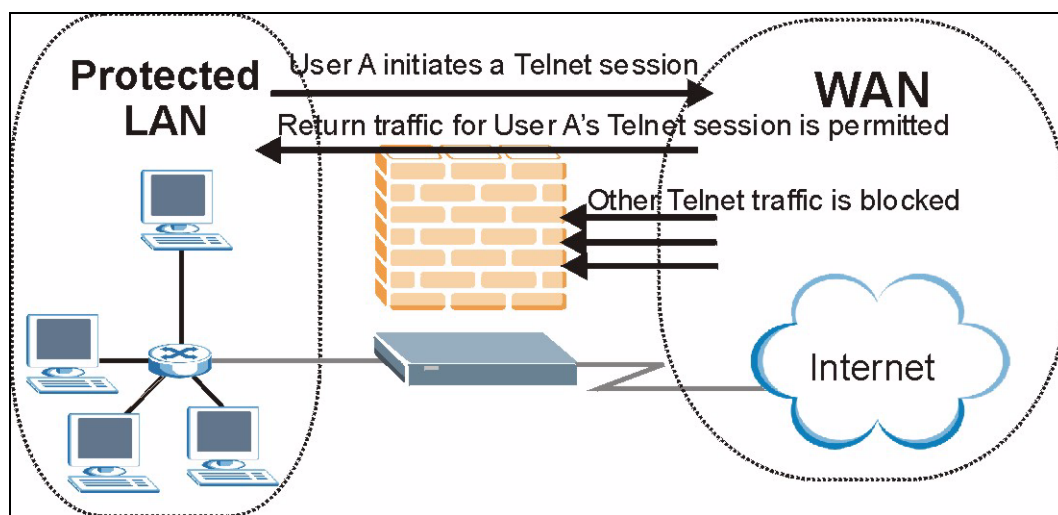
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking 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.

10.5 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 94 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.

10.5.1 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.

10.5.2 Stateful Inspection and the 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).

10.5.3 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).

10.5.4 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.

10.5.5 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.

10.6 Guidelines for Enhancing Security with Your Firewall

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

10.6.1 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.

10.7 Packet Filtering Vs Firewall

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

10.7.1 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.

10.7.1.1 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.

10.7.2 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.

10.7.2.1 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 11

Firewall Configuration

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

11.1 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 (Command Line Interpreter) commands provide limited configuration options and are only recommended for advanced users.

11.2 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
- LAN to DMZ
- WAN to LAN
- WAN to WAN/ Router
- WAN to DMZ
- DMZ to LAN
- DMZ to WAN
- DMZ to DMZ/ Router

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

- DMZ to WAN

By default, the ZyXEL Device's stateful packet inspection blocks 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.

- DMZ to LAN
- DMZ to DMZ/ Router

This prevents computers on the DMZ from communicating between networks or subnets connected to the DMZ interface and/or managing the ZyXEL Device.

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

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

For example, you may create rules to:

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

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

11.3 Rule Logic Overview

Note: Study these points carefully before configuring rules.

11.3.1 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.

11.3.2 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.

11.3.3 Key Fields For Configuring Rules

11.3.3.1 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.

11.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See [Section 11.8 on page 195](#) for more information on predefined services.

11.3.3.3 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?

11.3.3.4 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?

11.4 Connection Direction

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN. Rules for the DMZ work in a similar fashion.

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

11.4.1 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.

11.4.2 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 97 on page 188](#)). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen. Refer to the chapter on logs for details

11.5 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 10.1 on page 169](#) for more information.

Figure 95 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 DMZ	Permit	<input checked="" type="checkbox"/>
DMZ to WAN	Permit	<input checked="" type="checkbox"/>
LAN to DMZ	Permit	<input checked="" type="checkbox"/>
DMZ to LAN	Drop	<input checked="" type="checkbox"/>
WAN to WAN / Router	Drop	<input checked="" type="checkbox"/>
LAN to LAN / Router	Permit	<input type="checkbox"/>
DMZ to DMZ / Router	Drop	<input checked="" type="checkbox"/>

[Basic...](#)

The following table describes the labels in this screen.

Table 64 Firewall: General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	<p>Select this check box to have the ZyXEL Device firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology.</p> <p>Note: Allowing asymmetrical routes may let traffic from the WAN go directly to a LAN computer without passing through the router. See Appendix P on page 481 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.</p> <p>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, LAN to LAN / Router means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyXEL Device or the ZyXEL Device itself.</p>
Default Action	<p>Use the drop-down list boxes to select the default action that the firewall is take on packets that are traveling in the selected direction and do not match any of the firewall rules.</p> <p>Select Drop to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select Reject to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select Permit to allow the passage of the packets.</p>
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this button to display more information.
Basic...	Click this button to display less information.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

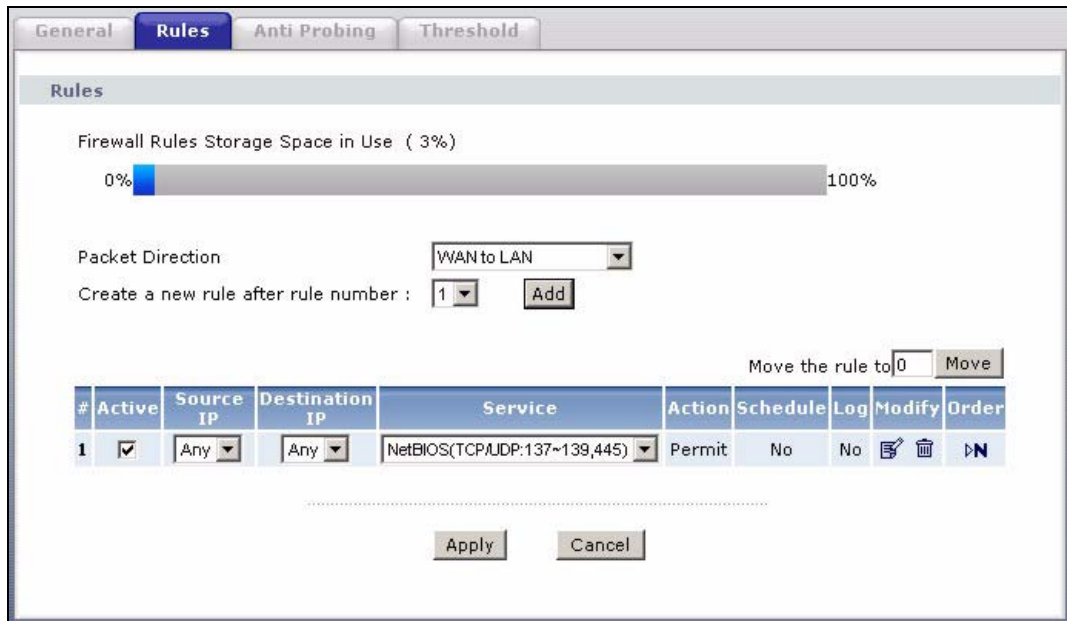
11.6 Firewall Rules Summary

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

Refer to [Section 10.1 on page 169](#) 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 96 Firewall Rules



The following table describes the labels in this screen.

Table 65 Firewall Rules

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyXEL Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click Add to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the General screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any .
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to Any .
Service	This drop-down list box displays the services to which this firewall rule applies. See Section 11.8 on page 195 for more information.

Table 65 Firewall Rules (continued)

LABEL	DESCRIPTION
Action	This field displays whether the firewall silently discards packets (Drop), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (Reject) or allows the passage of packets (Permit).
Schedule	This field tells you whether a schedule is specified (Yes) or not (No).
Log	This field shows you whether a log is created when packets match this rule (Yes) or not (No).
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Order	Click the Move icon to display the Move the rule to field. Type a number in the Move the rule to field and click the Move button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

11.6.1 Configuring Firewall Rules

Refer to [Section 10.1 on page 169](#) 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 97 Firewall: Edit Rule

Edit Rule 2

Active
 Action for Matched Packets: Permit

Source Address

Address Type: Any Address

Start IP Address: 0.0.0.0 Add >>

End IP Address: 0.0.0.0 Edit <<

Subnet Mask: 0.0.0.0 Delete

Source Address List

Any

Destination Address

Address Type: Any Address

Start IP Address: 0.0.0.0 Add >>

End IP Address: 0.0.0.0 Edit <<

Subnet Mask: 0.0.0.0 Delete

Destination Address List

Any

Service

Available Services

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

Add >>

Remove

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 0 hour 0 minute End 0 hour 0 minute

Log

Log Packet Detail Information.

Alert

Send Alert Message to Administrator When Matched.

Apply Cancel

The following table describes the labels in this screen.

Table 66 Firewall: Edit Rule

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select Drop to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select Reject to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select Permit to allow the passage of the packets.
Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: Single Address , Range Address , Subnet Address and Any Address .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click Add >> to add a new address to the Source or Destination Address box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click Edit << .
Delete	Highlight an existing source or destination address from the Source or Destination Address box above and click Delete to remove it.
Services	
Available/ Selected Services	Please see Section 11.8 on page 195 for more information on services available. Highlight a service from the Available Services box on the left, then click Add >> to add it to the Selected Services box on the right. To remove a service, highlight it in the Selected Services box on the right, then click Remove .
Edit Customized Service	Click the Edit Customized Services link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select All Day or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created or not. Go to the Log Settings page and select the Access Control logs category to have the ZyXEL Device record these logs.
Alert	
Send Alert Message to Administrator When Matched	Select the check box to have the ZyXEL Device generate an alert when the rule is matched.

Table 66 Firewall: Edit Rule (continued)

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

11.6.2 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. For further information on these services, please read [Section 11.8 on page 195](#). 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 10.1 on page 169](#) for more information.

Figure 98 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 67 Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to a screen where you can configure or edit a customized service. See Section 11.6.3 on page 191 for more information.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (TCP , UDP or TCP/UDP) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click Back to return the Firewall Edit Rule screen.

11.6.3 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 10.1 on page 169](#) for more information.

Figure 99 Firewall: Configure Customized Services

The following table describes the labels in this screen.

Table 68 Firewall: Configure Customized Services

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

11.7 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 100 Firewall Example: Rules

General **Rules** Anti Probing 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 101 Edit Custom Port Example

Config

Service Name MyService

Service Type TCP/UDP

Port Configuration

Type Single Port Range

Port Number From 123 To 123

Apply Cancel Delete

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

Figure 102 Firewall Example: Edit Rule: Destination Address

The screenshot shows the 'Edit Rule 1' configuration window. At the top, the rule is 'Active' and the action is 'Permit'. The 'Source Address' section is set to 'Any Address' with a start and end IP of 0.0.0.0 and a subnet mask of 0.0.0.0. The 'Destination Address' section is set to 'Range Address' with a start IP of 10.0.0.10 and an end IP of 10.0.0.15, and a subnet mask of 0.0.0.0. The 'Service' section is partially visible at the bottom.

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

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

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

Figure 103 Firewall Example: Edit Rule: Select Customized Services

Edit Rule 2

Active
Action for Matched Packets: **Permit**

Source Address

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

Source Address List: **Any**

Buttons: Add >>, Edit <<, Delete

Destination Address

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

Destination Address List: **10.0.0.10 - 10.0.0.15**

Buttons: Add >>, Edit <<, Delete

Service

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

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

Buttons: Add >>, Remove

[Edit Customized Services](#)

Schedule

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

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

Log:
 Log Packet Detail Information.

Alert:
 Send Alert Message to Administrator When Matched.

Buttons: **Apply**, Cancel

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

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

Figure 104 Firewall Example: Rules: MyService

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

11.8 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see [Section 11.6.1 on page 187](#)) displays all predefined services that the ZyXEL Device already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “(DNS)”. **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom service ports may also be configured using the **Edit Customized Services** function discussed previously.

Table 69 Predefined Services

SERVICE	DESCRIPTION
AIM/NEW_ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.

Table 69 Predefined Services (continued)

SERVICE	DESCRIPTION
H.323(TCP:1720)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IPSEC_TRANSPORT/ 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.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS (TCP/ UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.

Table 69 Predefined Services (continued)

SERVICE	DESCRIPTION
SSDP(UDP:1900)	Simple Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using DUDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(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.

11.9 Anti-Probing

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. The 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.

Internet Control Message Protocol (ICMP) 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.

Refer to [Section 10.1 on page 169](#) for more information.

Click **Security > Firewall > Anti Probing** to display the screen as shown.

Figure 105 Firewall: Anti Probing

The following table describes the labels in this screen.

Table 70 Firewall: Anti Probing

LABEL	DESCRIPTION
Respond to PING on	The ZyXEL Device does not respond to any incoming ping requests when Disable is selected. Select the interface which you want to reply to incoming ping requests.
Do Not Respond to Requests for Unauthorized Services.	Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. By default this option is not selected and the ZyXEL Device will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the ZyXEL Device's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyXEL Device reacts based on the corresponding firewall policy to send a TCP reset packet for a blocked TCP packet or an ICMP port-unreachable packet for a blocked UDP packets or just drop the packets without sending a response packet.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

11.10 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 11.10.3 on page 200](#) to configure thresholds.

11.10.1 Threshold Values

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

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

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

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

11.10.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state—the TCP three-way handshake has not yet been completed (see [Figure 91 on page 172](#)). For UDP, "half-open" means that the firewall has detected no return traffic.

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

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

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

11.10.2.1 TCP Maximum Incomplete and Blocking Time

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

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

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

11.10.3 Configuring Firewall Thresholds

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

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

Figure 106 Firewall: Threshold

The following table describes the labels in this screen.

Table 71 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 71 Firewall: Threshold (continued)

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

CHAPTER 12

Anti-Virus Packet Scan

This chapter introduces and shows you how to configure the anti-virus packet scan.

12.1 Overview

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

12.1.1 Types of Computer Viruses

The following table describes some of the common computer viruses.

Table 72 Common Computer Virus Types

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extent renders the infected computer inoperable.
Macro Virus	Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macro viruses spread more rapidly than other types of viruses as data files are often shared on a network.
E-mail Virus	E-mail viruses are malicious programs that spread through e-mail. These can infect your computer even if you do not read the e-mail messages.

12.2 Signature-Based Virus Scan

The “signature-based” approach is the most common way to detect the presence of viruses. Signature-based anti-virus scanning consists of two key components: a pattern file that contains the signatures for known viruses and a scanning engine.

Signatures are byte patterns that are unique to a particular virus. These signatures are stored in a pattern file. The scanning engine compares the files with the signatures in the pattern file.

For maximum protection, you must keep the pattern file up-to-date.

12.2.1 Computer Virus Infection and Prevention

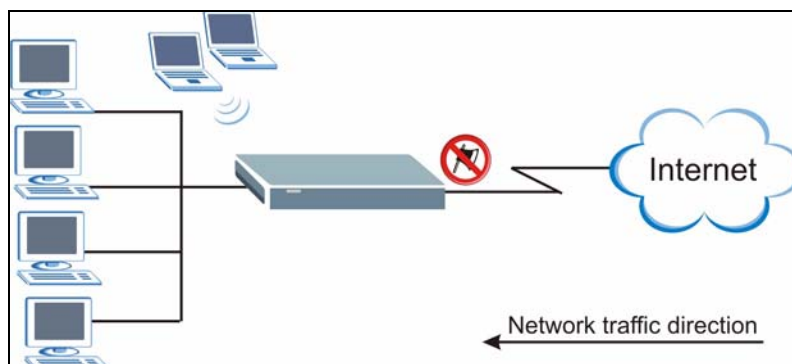
The follow describes a simplistic life cycle of a computer virus.

- 1 A computer gets a copy of a virus from an unknown source (such as the Internet, e-mail, file sharing or any removable storage media). The virus is harmless until the execution of an infected program.
- 2 The virus spreads to other files and programs on the computer.
- 3 The infected files are unintentionally sent to another computer thus starting the spread of the virus.
- 4 Once the virus is spread through the network, the number of infected networked computers can grow exponentially.
- 5 To prevent the spread of viruses, you need to install host-based anti-virus software on a computer or buy an anti-virus system.

12.3 Introduction to the ZyXEL Device Anti-virus Packet Scan

The ZyXEL Device has an integrated signature-based anti-virus packet scan. Set up the ZyXEL Device between your local network and the Internet. This way the ZyXEL Device can scan incoming traffic to your local network from the Internet. Thus the ZyXEL Device helps stop threats at the network edge before they reach the local host computers.

Figure 107 ZyXEL Device Anti-virus Application



Your ZyXEL Device is able to scan the following network traffic types for viruses:

- HTTP (Hyper Text Transfer Protocol)
This is the most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers.
- Mail messages (SMTP, POP3)
- FTP (File Transfer Protocol)

This 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.

Note: The anti-virus packet scan on the ZyXEL Device offers the first defense against possible virus attacks on your network. It is not a replacement of the anti-virus client software that you may install on network computers.

12.3.1 How the ZyXEL Device Virus Scan Works

The following describes the virus scanning process on the ZyXEL Device.

- 1 The ZyXEL Device first identifies the packet types (SMTP, POP3, HTTP and FTP through standard ports only) from the network traffic.
- 2 If the packets are not session connection setup packets (such as SYN, ACK and FIN), the ZyXEL Device records the sequence of the packets.
- 3 The scanning engine scans the content of the packet for virus.
- 4 If a virus pattern is matched, the ZyXEL Device “cleans” the virus by deleting the infected packet and alerts the intended computer user(s).

Note: Since the ZyXEL Device “destroys” a file by deleting the infected portion of the file content, you cannot open the file.

12.3.2 Limitations of the ZyXEL Device Packet Scan

The ZyXEL Device does not scan the following types of file for virus:

- Compressed or zipped files
- Simultaneous file downloads (for example, when you use the FlashGet download program).
- When a virus is detected, an alert message is displayed in Microsoft Windows-based operation systems only.¹

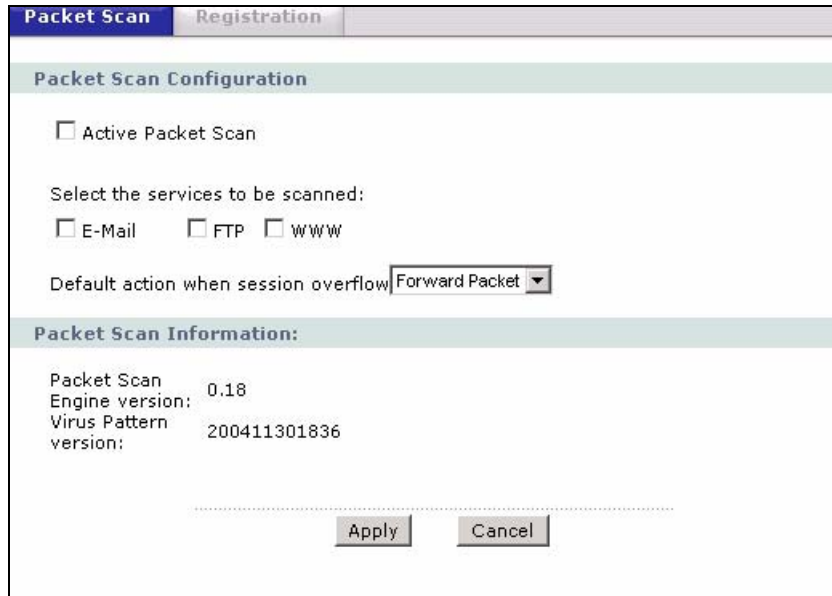
12.4 Anti-Virus Packet Scan Configuration

Note: Before you can use the anti-virus packet scan on the ZyXEL Device, you must register for the anti-virus service in the **Registration and Virus Information Update** screen (see the [Section 12.5 on page 207](#) section for more information).

1. For Windows 98/Me, refer to the antivirus supplement for requirements.

Click **Security > AntiVirus** to display the configuration screen as shown next.

Figure 108 Anti-Virus: Packet Scan



The following table describes the labels in this screen.

Table 73 Anti-Virus: Packet Scan

LABEL	DESCRIPTION
Packet Scan Configuration	
Active	Select this check box to enable the anti-virus packet scan on the ZyXEL Device. Clear this check box to disable it. Before you activate the anti-virus packet scan, register for the service in the Registration and Virus Information Update screen.
Choose which application to be scanned:	
E-Mail	Select this option to scan incoming/outgoing e-mail content for viruses.
FTP	Select this option to scan FTP traffic for viruses.
HTTP	Select this option to scan HTTP traffic for viruses.
Default action when session overflow	Select whether to allow passage of (Forward Packet) or silently discard (Block Packet) the packets of new connections when the maximum number of opened connections is reached (default is 300 connections at a time).
Packet Scan Information	
Packet Scan Engine Version	This read-only field displays the version of the scanning engine on the ZyXEL Device.
Virus Pattern Version	This read-only field displays the version number of the virus pattern. It is recommended that you update the pattern file regularly in the Registration and Virus Information Update screen (refer to the Section 12.5 on page 207 section for more information).
Back	Click Back to return to the previous screen.

Table 73 Anti-Virus: Packet Scan (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

12.5 Registration and Online Update

Use the **Registration and Virus Information Update** screen to register for and activate the anti-virus packet scan feature on the ZyXEL Device. You can also configure a schedule for the ZyXEL Device to automatically update the virus pattern file in this screen.

Click **Anti Virus > Registration > Virus Information Update** to display the screen as shown.

Note: The ZyXEL Device automatically restarts after the virus scan update is complete.

Figure 109 Anti-Virus: Registration and Virus Information Update

The following table describes the labels in this screen.

Table 74 Anti-Virus: Registration and Virus Information Update

LABEL	DESCRIPTION
Registration	You must register for the anti-virus service before you can use the packet scan feature on the ZyXEL Device. Registering for the service allows you to activate packet scan and download the virus pattern file. Click Registration and follow the online instructions to register. Refer to the Section on page 496 appendix for more information.
Activation	After you have successfully registered for the anti-virus service, click Activate to enable and start using the anti-virus feature. This also sets the ZyXEL Device to automatically update the pattern file.
Virus Information Update	Set the fields below to configure the ZyXEL Device to automatically update the pattern file.
Update Schedule	This drop-down menu is used to configure the frequency of the automatic pattern file update. Choices are 1 hr , 12 hr and 24 hr .
Manually Update Virus Information	Click Update Now to download and update to the latest pattern file.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

12.5.1 Updating the Anti-Virus Packet Scan

Follow the steps below to update the virus scan on the ZyXEL Device manually.

Note: Do not turn off the ZyXEL Device while the virus scan update is in progress!

- 1 In the **Registration and Virus Information Update** screen, click **Update Now**. An update progress screen displays as shown.

Figure 110 Virus Scan Update in Progress



- 2 After the virus scan update is successful, a screen displays as shown.

Figure 111 Virus Scan Update Successful



The ZyXEL Device automatically restarts after the virus scan update is complete.

CHAPTER 13

Content Filtering

This chapter covers how to configure content filtering.

13.1 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.

13.2 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 112 Content Filter: Keyword

The screenshot shows a web-based configuration interface for content filtering. It features three tabs: 'Keyword', 'Schedule', and 'Trusted'. The 'Keyword' tab is active. The main content area is titled 'Keyword' and contains a checked checkbox for 'Active Keyword Blocking'. Below this, a text box labeled 'Block Websites that contain these keywords in the URL :' contains the word 'bad'. There are 'Delete' and 'Clear All' buttons below the text box. At the bottom of the main area, there is a 'Keyword' input field and an 'Add Keyword' button. At the very bottom of the window, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 75 Content Filter: Keyword

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

13.3 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 113 Content Filter: Schedule

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

The following table describes the labels in this screen.

Table 76 Content Filter: Schedule

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

13.4 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 114 Content Filter: Trusted

The following table describes the labels in this screen.

Table 77 Content Filter: Trusted

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

CHAPTER 14

Content Access Control

This chapter gives some background information on Content Access Control and explains how to get started with the ZyXEL Device Content Access Control.

14.1 Content Access Control Overview

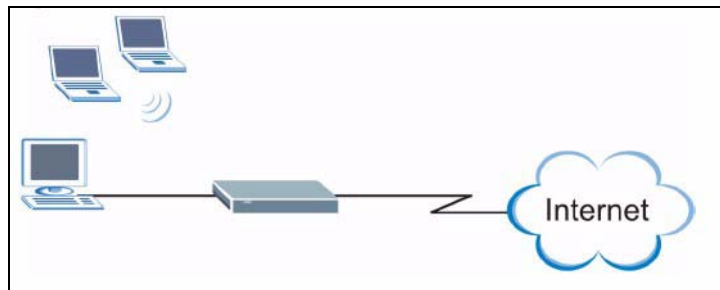
Content Access Control (CAC) lets a LAN administrator control a LAN user's Internet access privileges by blocking services that you specify. The administrator can create user groups with access restrictions and set up user accounts (with a login name and password) for each person (user) on the network. The user accounts are associated to a user group. Each person must log into the system before they can gain access to the Internet.

14.1.1 Content Access Control WLAN Application

You can control LAN user Internet access by having an administrator configure Content Access Control on the ZyXEL Device.

The administrator must create user groups and accounts (each person (user) on the network). Each person must log into the system before they can gain access to the Internet. Each user group will hold the details (access rights and privileges and time schedule) for the associated user accounts. The ZyXEL Device enforces these access restrictions.

Figure 115 Content Access Control with WLAN Application



14.1.2 Configuration Steps

To activate and set up Content Access Control on the ZyXEL Device, you must do the following tasks.

- 1 Create four user groups with access restrictions and schedule.
- 2 Create user accounts and associate the user accounts to a user group.

14.2 Activating CAC and Creating User Groups

From the main menu click **Security > Content Access Control** and **General** to open the configuration screen.

Use this screen to activate Content Access Control and set up the four user groups.

Note: You must set up all four user groups.

Figure 116 Content Access Control: General

The following table describes the labels in this screen.

Table 78 Content Access Control: General



LABEL	DESCRIPTION
Enable Content Access Control	Select the check box to allow the LAN administrator to have control over a LAN user's Internet access.
Idle Timeout	Type the time in minutes that elapses before the ZyXEL Device automatically terminates the Internet session. The default time is 10 minutes.
Group List	These groups are used in conjunction with content filtering to decide which web pages cannot be accessed by the user. You can set up to four user groups.
Group Name	Enter the name of a user group for identification purposes.
Restrictions	Use the links below to configure the access restrictions for the user group.
Time	Click the Edit () icon to set up the time allowances, start times and end times of the day(s) when access is allowed.

Table 78 Content Access Control: General (continued)

LABEL	DESCRIPTION
Service	Click Edit to select the services you wish to block access for a user group.
Web Browsing	Click Edit to specify the web site category(ies) and/or key words in a web site address you wish to block access for a user group. Click the Diagnose icon () to test the access privilege on a specified web site address.
Content Filtering Service	Click Register to go to a web site where you can register for category-based content filtering (using an external database). You can use a trial application or register your iCard's PIN. Refer to the web site's on-line help for details. Note: Refer to the Section on page 496 appendix on more information on device and service registration. You can also manage your registration status or view content filtering reports after you register this device in the service registration web site. Note: The web site displays a registration successful web page. It may take up to another ten minutes for content filtering to be activated. See on how to check the content filtering activation. Click Activate to begin the content filtering service now.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

14.2.1 Configuring Time Schedule

To set up the time schedule for each user group, click **Edit** under **Time** in the **Content Access Control-General** screen. A screen displays as shown next.

Figure 117 Control Access Control: General: Time Scheduling

Time Scheduling

Allow hr min access from to everyday

Allow Custom Daily Access

	Unlimited	Time Budget Left	Start Time	End Time
Monday	<input type="checkbox"/>	<input type="text" value="0"/> hr <input type="text" value="0"/> min	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
Tuesday	<input type="checkbox"/>	<input type="text" value="0"/> hr <input type="text" value="0"/> min	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
Wednesday	<input type="checkbox"/>	<input type="text" value="0"/> hr <input type="text" value="0"/> min	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
Thursday	<input type="checkbox"/>	<input type="text" value="0"/> hr <input type="text" value="0"/> min	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
Friday	<input type="checkbox"/>	<input type="text" value="0"/> hr <input type="text" value="0"/> min	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
Saturday	<input type="checkbox"/>	<input type="text" value="0"/> hr <input type="text" value="0"/> min	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
Sunday	<input type="checkbox"/>	<input type="text" value="0"/> hr <input type="text" value="0"/> min	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>

Back Apply Cancel

The following table describes the labels in this screen.

Table 79 Control Access Control: General: Time Scheduling

LABEL	DESCRIPTION
Time Scheduling	Select the first radio button to allow everyday access at the same times to the Internet. Type the interval time allowance (number of hours and minutes). Select the start and end times from the drop-down list boxes to configure the period during the day when access is allowed. Select Allow Custom Daily Access to configure time allowances, start times and end times for each day.
Unlimited	Select the check box for the day(s) that you do not want any time restrictions for user Internet access.
Time Budget Left	Type the number of hours (0 to 23) and minutes (0 to 59) to allow Internet access of unblocked sites. Note: If you want to allow twenty-four hour access, you should select the Unlimited check box.
Start Time	Select from the drop-down list box a time during the day when a user can begin accessing unblocked sites.
End Time	Select from the drop-down list box a time during the day when a user can no longer access unblocked sites. The time allowance must be less than or equal to the period from the start time to the end time. Note: User access will be denied after the End Time for that day even if the time allowance has not run out.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

14.2.2 Configuring Services

To customize services for each user group, click **Edit** under **Services** for that user group in the **Content Access Control: General** screen.

Figure 118 Content Access Control: General: Services

The following table describes the labels in this screen.

Table 80 Content Access Control: General: Services

LABEL	DESCRIPTION
Service to be Blocked	
Available services	Select a service from the list and click the >> button to have the service blocked on a weekday (Monday to Friday) or to have the service blocked on a day in the weekend (Saturday or Sunday). These services will be blocked according to the settings you configure in Time Scheduling screen.
Blocked Services	This box shows all the services that you want to block during the specified time for the user group. Click the << button to remove a service from the box.
Customized Services	A customized service is a service that is not available in the pre-defined Available Services list and you must define using the next two fields.
Type	Services are either TCP and/or UDP . Select from either TCP or UDP .
Port Number	Enter a port number or a range of port numbers to define the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.
Add	Click Add to add a service to be blocked to the Blocked Services box.
Clear All	Click Clear All to empty the Blocked Services box.
Back	Click Back to return to the previous screen.

Table 80 Content Access Control: General: Services (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

14.2.2.1 Available Services

The **Available Services** list box in the **Services** screen displays some predefined services that the ZyXEL Device supports. The following table shows a list of services that can be configured. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “(DNS)”. (UDP/TCP:53) means UDP port 53 and TCP port 53.

Table 81 Available Services

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

Table 81 Available Services (continued)

SERVICE	DESCRIPTION
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
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.
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.

14.2.3 Configuring Web Site Filters

To enable content filtering and to configure URL keyword blocking for a user group, click **Edit** under **Web Browsing** in the **Content Access Control: General** screen. A screen displays as shown next.

Figure 119 Content Access Control: General: Web Site Filter

The following table describes the labels in this screen.

Table 82 Content Access Control: General: Web Site Filter

LABEL	DESCRIPTION
Pre-defined Web Content Categories	Enable Pre-defined Web Content Categories to have the ZyXEL Device check an external database to find to which category a requested web page belongs. The ZyXEL Device then blocks or forwards access to the web page depending on the configuration of the rest of this page.
Enable	This field is applicable when you have successfully registered for and activated the content filtering services. Refer to the User's Guide for more information. Select this option to start using the external content filtering service on the ZyXEL Device.

Table 82 Content Access Control: General: Web Site Filter (continued)

LABEL	DESCRIPTION
Log Matched Web Site	Select this option to record attempts to access prohibited web pages.
Select Blocked Categories	Use this section to prevent users from accessing web pages that match the categories that you select below.
Select All	Select this check box to restrict access to all site categories listed below.
Clear All	Select this check box to clear the selected categories below.
Adult/Mature Content	Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children.
Pornography	Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Sex Education	Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement.
Intimate Apparel/ Swimsuit	Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered.
Nudity	Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals.
Alcohol/Tobacco	Selecting this category excludes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products.
Illegal/Questionable	Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers.
Gambling	Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements).
Violence/Hate/Racism	Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics.
Weapons	Selecting this category excludes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use.

Table 82 Content Access Control: General: Web Site Filter (continued)

LABEL	DESCRIPTION
Abortion	Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.
Arts/Entertainment	Selecting this category excludes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment.
Business/Economy	Selecting this category excludes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services).
Cult/Occult	Selecting this category excludes pages that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers and satanic or supernatural beings.
Illegal Drugs	Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
Education	Selecting this category excludes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups.
Cultural Institutions	Selecting this category excludes pages sponsored by cultural institutions, or those that provide information about museums, galleries, and theaters (not movie theaters). It includes groups such as 4H and the Boy Scouts of America.
Financial Services	Selecting this category excludes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services.
Brokerage/Trading	Selecting this category excludes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news.
Games	Selecting this category excludes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways.
Government/Legal	Selecting this category excludes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities.
Military	Selecting this category excludes pages that promote or provide information on military branches or armed services.
Political/Activist Groups	Selecting this category excludes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities.

Table 82 Content Access Control: General: Web Site Filter (continued)

LABEL	DESCRIPTION
Health	Selecting this category excludes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition.
Computers/Internet	Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies.
Hacking/Proxy Avoidance	Pages providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server.
Search Engines/Portals	Selecting this category excludes pages that support searching the Internet, indices, and directories.
Web Communications	Selecting this category excludes pages that allow or offer Web-based communication via e-mail, chat, instant messaging, message boards, etc.
Job Search/Careers	Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers.
News/Media	Selecting this category excludes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories.
Personals/Dating	Selecting this category excludes pages that promote interpersonal relationships.
Reference	Selecting this category excludes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information.
Chat/Instant Messaging	Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads.
Email	Selecting this category excludes pages offering web-based email services, such as online email reading, e-cards, and mailing list services.
Newsgroups	Selecting this category excludes pages that offer access to Usenet news groups or other messaging or bulletin board systems.
Religion	Selecting this category excludes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft (Cult/Occult) or atheist beliefs (Political/Activist Groups).
Shopping	Selecting this category excludes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons).
Auctions	Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements.
Real Estate	Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties.

Table 82 Content Access Control: General: Web Site Filter (continued)

LABEL	DESCRIPTION
Society/Lifestyle	Selecting this category excludes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category.
Gay/Lesbian	Selecting this category excludes pages that provide information, promote, or cater to gay and lesbian lifestyles. This does not include pages that are sexually oriented.
Restaurants/Dining/ Food	Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes.
Sports/Recreation/ Hobbies	Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting.
Travel	Selecting this category excludes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
Vehicles	Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts.
Humor/Jokes	Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating.
Streaming Media/MP3	Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including pages that provide downloads for such viewers.
Software Downloads	Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge.
Pay to Surf	Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.
For Kids	Selecting this category excludes pages designed specifically for children.
Web Advertisements	Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements.
Web Hosting	Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services.
More/Basic	Click more... to see an expanded list of categories, or click basic... to see a smaller list.
Keyword Blocking	Select the Enable check box to block the URL containing the keywords in the keyword list.
Block Websites that contain these keywords in the URL	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.
Delete	Select a keyword from the keyword list and then click Delete to remove this keyword from the list.
Clear All	Click Clear All to empty the keyword list.

Table 82 Content Access Control: General: Web Site Filter (continued)

LABEL	DESCRIPTION
Keyword	Type a keyword in the Keyword field and then click Add Keyword to add a keyword to the list of keywords. The list of keywords that will be inaccessible to computers on your LAN once you enable URL keyword blocking.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

14.2.4 Testing Web Site Access Privileges

To check the access restrictions of a web site, click **Diagnose** under **Web Browsing** in the **Content Access Control: General** screen. A screen displays as shown next.

The ZyXEL Device first checks the web site address for the specified keyword(s) to block. If the web site address does not contain any blocking keywords, the ZyXEL Device then checks the rating information on the remote content filtering database (provided that you have successfully registered for and activated this service) and block or allow access depending on the rating information of the web site.

Figure 120 Content Access Control: General: Diagnose

The following table describes the labels in this screen.

Table 83 Content Access Control: General: Diagnose

LABEL	DESCRIPTION
Test Web Site Attribute	
Test Result	This field displays the web site address check result.
Test if web site is blocked	Enter the URL or web site address in the field provided and click Test to check the access restrictions of the web site.
Test	This button is applicable when you have either activated and/or configured keyword blocking or registered and activated the content filtering service. Click Test to check the access privileges of the specified web site address.
Back	Click Back to return to the previous screen.
Cancel	Click Cancel to return to the previously saved settings.

14.3 User Account Setup

With Content Access Control, the ZyXEL Device requires LAN users to login with valid username and password before they are allowed to access the Internet.

Use the **User Profile** screen to set up user accounts. From the main menu click **Security > Content Access > User Profile** to display the screen as shown next.

Figure 121 Content Access Control: User Profiles

here.' At the bottom of the screen are two buttons: 'Apply' and 'Cancel'."/>

Index	Username	Password	Category
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

If you want to add more user profiles, please click [here](#).

Apply Cancel

The following table describes the labels in this screen.

Table 84 Content Access Control: User Profiles

LABEL	DESCRIPTION
Index	This field displays the index number.
Username	Enter the user name for this account.
Password	Enter a password associated to the user name above.
Category	Select a user group from the drop-down list box to associate this user account to the user group. The drop-down list box displays the name of the user group you configure in the General screen.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

14.4 User Online Status

To view the online status of each user, click **Security > Content Access Control > Online Status** to display the screen as shown.

Figure 122 Content Access Control: Online Status

Index	Username	Category	Time Left	On-Line
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
25				
26				
27				
28				
29				
30				
31				
32				

The following table describes the labels in this screen.

Table 85 Content Access Control: Online Status

LABEL	DESCRIPTION
Index	This field displays the index number.
Username	This field displays the username (up to 30 characters) for this user profile.
Group	This field displays the name of the associated user group.
Time Left	This field displays the amount of time that you have before the ZyXEL Device logs you out and terminates your Internet access. This time depends on the time allowance configured in Time Scheduling screen. By using the + or – buttons, the administrator can increase or decrease the time left in 15 minute increments without re-configuring the time allowances.
On-Line	This field displays Yes if a user is currently on-line. This field displays Ready if a user is allowed to access the Internet at the moment and is currently not on-line. This field displays No if a user is not allowed to access the Internet at the moment and is currently not on-line.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

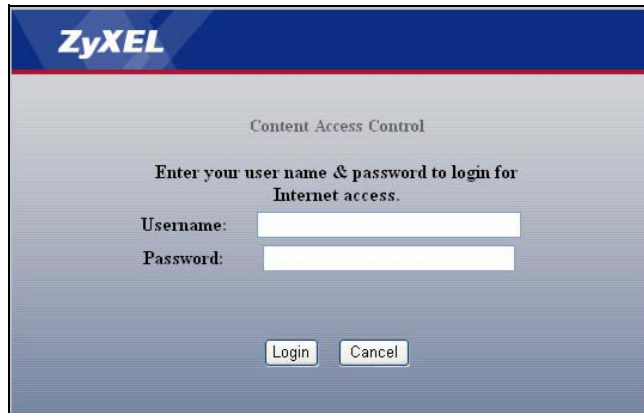
14.5 Content Access Control Logins

The following sections describe the user and administrator login experience.

14.5.1 User Login

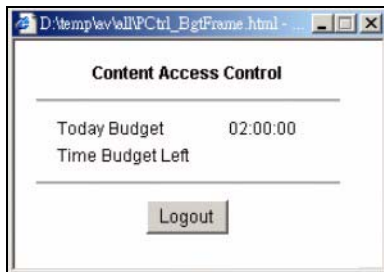
- 1 Once the initial configuration is complete, a computer on the network cannot gain Internet access without first logging into the ZyXEL Device.
- 2 When you attempt to access a website, you are directed to the ZyXEL Device's user login screen.

Figure 123 Content Access Control: User Login Screen



- 3 After you enter your login name and password the ZyXEL Device checks the access profile and begins enforcing the access control restriction as defined by the administrator.
- 4 The access privileges remain in force until you log out.
- 5 After a successful login, the system launches a small pop-up window that displays the remaining budget time and a logout button.

Figure 124 Content Access Control: User Logout Screen



There are four ways to be logged out of the system.

- Click the **Logout** button in the user logout screen.
- The idle timeout triggers the logout (the default is ten minutes).
- The access time allowance budget reaches zero and triggers the logout.
- The system clock reaches the end time for the user's account and triggers the logout.

14.5.2 Administrator Login

The administrator can log into the system.

- The administrator opens their browser and is directed to the ZyXEL Device user login page (this is the same as the user login).
- The administrator enters “admin” as the username and the system password.
- The system administrator main menu screen opens.

CHAPTER 15

Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

15.1 VPN Overview

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

15.1.1 IPSec

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

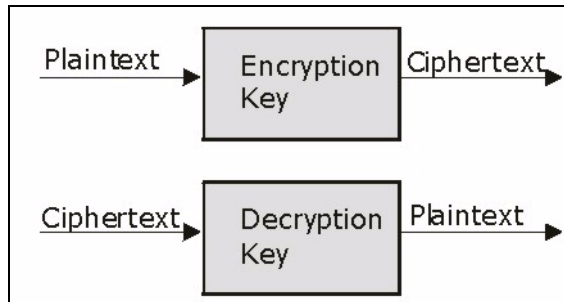
15.1.2 Security Association

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

15.1.3 Other Terminology

15.1.3.1 Encryption

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

Figure 125 Encryption and Decryption

15.1.3.2 Data Confidentiality

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

15.1.3.3 Data Integrity

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

15.1.3.4 Data Origin Authentication

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

15.1.4 VPN Applications

The ZyXEL Device supports the following VPN applications.

- Linking Two or More Private Networks Together

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

- Accessing Network Resources When NAT Is Enabled

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

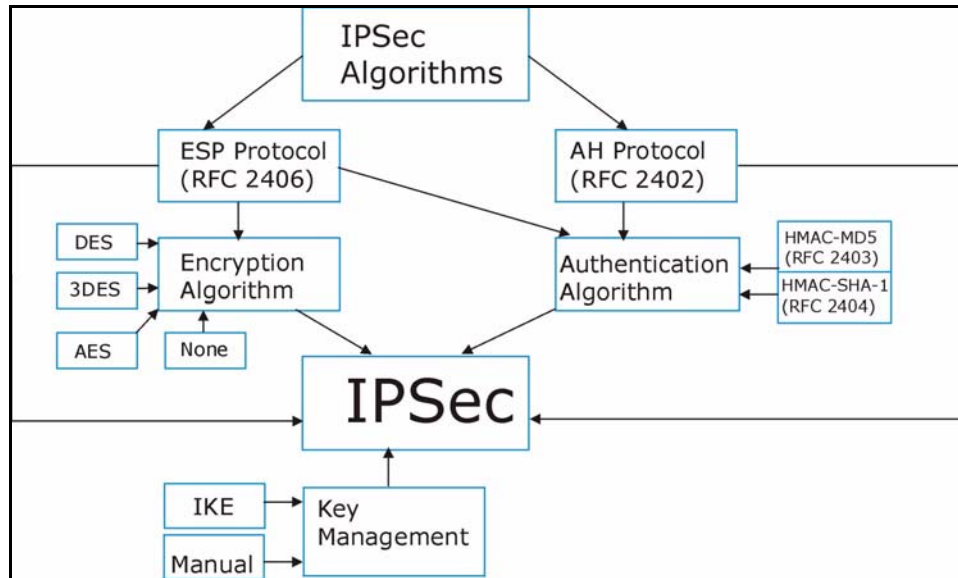
- Unsupported IP Applications

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

15.2 IPsec Architecture

The overall IPsec architecture is shown as follows.

Figure 126 IPsec Architecture



15.2.1 IPsec Algorithms

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

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

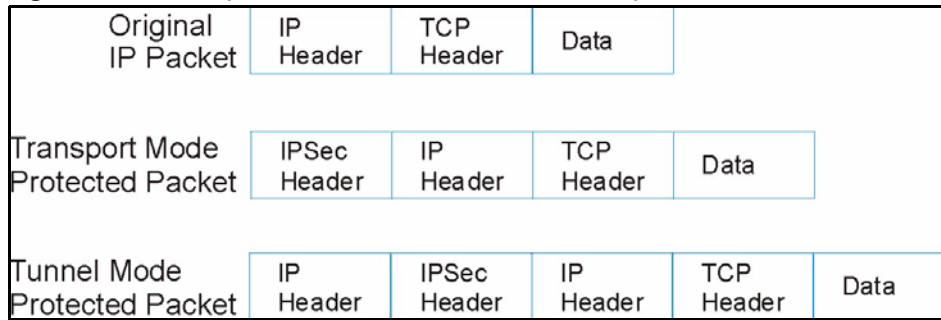
The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols. Please see [Section 16.2 on page 239](#) for more information.

15.2.2 Key Management

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

15.3 Encapsulation

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

Figure 127 Transport and Tunnel Mode IPSec Encapsulation

15.3.1 Transport Mode

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

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

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

15.3.2 Tunnel Mode

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

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

15.4 IPSec and NAT

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

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

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

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

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

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

Table 86 VPN and NAT

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

CHAPTER 16

VPN Screens

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

16.1 VPN/IPSec Overview

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

16.2 IPSec Algorithms

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

16.2.1 AH (Authentication Header) Protocol

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

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

16.2.2 ESP (Encapsulating Security Payload) Protocol

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

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

Table 87 AH and ESP

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

16.3 My IP Address

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

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

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

16.4 Secure Gateway Address

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

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

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

16.4.1 Dynamic Secure Gateway Address

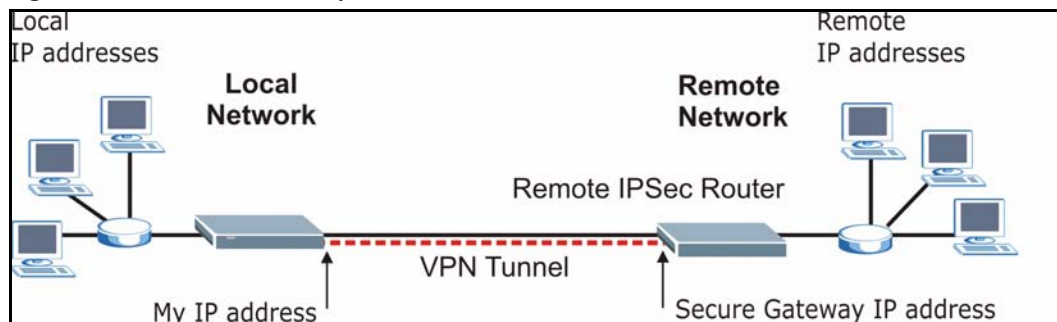
If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (see [Section 16.18 on page 262](#) for configuration examples).

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

16.5 VPN Setup Screen

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

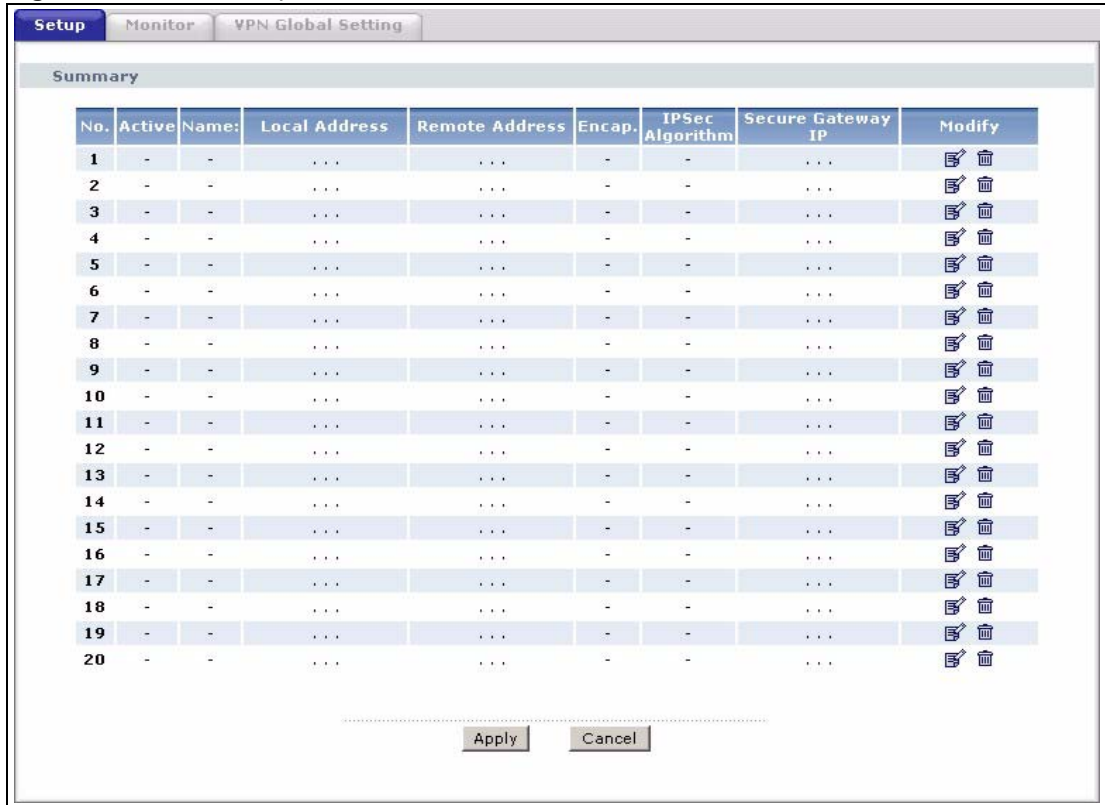
Figure 128 IPsec Summary Fields



Local and remote IP addresses must be static.

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

Figure 129 VPN Setup



The following table describes the fields in this screen.

Table 88 VPN Setup

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

Table 88 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 N/A when the Secure Gateway Address field displays 0.0.0.0. In this case only the remote IPSec router can initiate the VPN.</p> <p>The same (static) IP address is displayed twice when the Remote Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Single.</p> <p>The beginning and ending (static) IP addresses, in a range of computers are displayed when the Remote Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Range.</p> <p>A (static) IP address and a subnet mask are displayed when the Remote Address Type field in the VPN-IKE (or VPN-Manual Key) screen is configured to Subnet.</p>
Encap.	This field displays Tunnel or Transport mode (Tunnel is the default selection).
IPSec Algorithm	<p>This field displays the security protocols used for an SA.</p> <p>Both AH and ESP 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 0.0.0.0 when you configure the Secure Gateway Address field in the VPN-IKE screen to 0.0.0.0 .
Modify	<p>Click the edit icon to go to the screen where you can edit the VPN configuration.</p> <p>Click the delete icon to remove an existing VPN configuration.</p>
Back	Click Back to return to the previous screen.

16.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL Device automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see [Section 16.12 on page 252](#) for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a ZyXEL Device-compatible keep alive feature enabled in order for this feature to work.

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

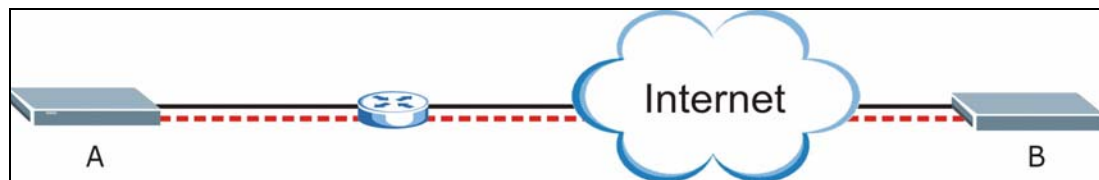
When there is outbound traffic with no inbound traffic, the ZyXEL Device automatically drops the tunnel after two minutes.

16.7 VPN, NAT, and NAT Traversal

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

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

Figure 130 NAT Router Between IPsec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPsec routers because the NAT router changes the header of the IPsec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPsec packet. The NAT router forwards the IPsec packet with the UDP port 500 header unchanged. In [Figure 130 on page 244](#), when IPsec router A tries to establish an IKE SA, IPsec router B checks the UDP port 500 header, and IPsec routers A and B build the IKE SA.

For NAT traversal to work, you must:

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

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

Table 89 VPN and NAT

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

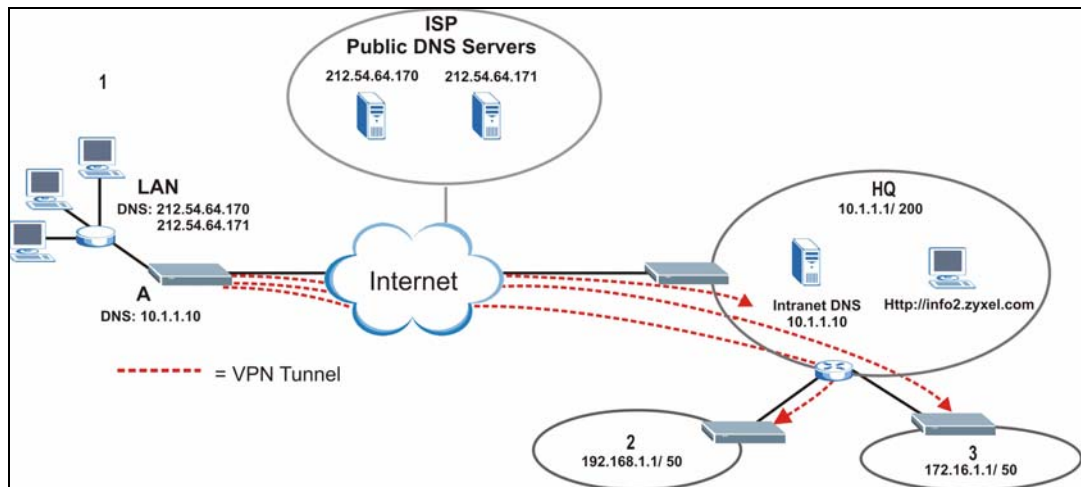
Y* - This is supported in the ZyXEL Device if you enable NAT traversal.

16.8 Remote DNS Server

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

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

Figure 131 VPN Host using Intranet DNS Server Example



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

16.9 ID Type and Content

With aggressive negotiation mode (see [Section 16.12.1 on page 253](#)), the ZyXEL Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyXEL Device from IPSec routers with dynamic IP addresses (see [Section 16.18 on page 262](#) for a telecommuter configuration example).

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

With main mode (see [Section 16.12.1 on page 253](#)), the ID type and content are encrypted to provide identity protection. In this case the ZyXEL Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL Device can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see [Section 16.13 on page 254](#)). The ID type and content act as an extra level of identification for incoming SAs.

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

Table 90 Local ID Type and Content Fields

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

Table 91 Peer ID Type and Content Fields

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

16.9.1 ID Type and Content Examples

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

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

Table 92 Matching ID Type and Content Configuration Example

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

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

Table 93 Mismatching ID Type and Content Configuration Example

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

16.10 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see [Section 16.12 on page 252](#) for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

16.11 Editing VPN Policies

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

Figure 132 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'. Below these are 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:** Contains 'Local Address Type' (Single), 'IP Address Start' (0.0.0.0), and 'End / Subnet Mask' (0.0.0.0).
- Remote:** Contains 'Remote Address Type' (Single), 'IP Address Start' (0.0.0.0), and 'End / Subnet Mask' (0.0.0.0).
- Address Information:** Contains fields for 'Local ID Type' (IP), 'Content', 'Local ID Type' (12345678), 'Content' (factory@auto.gen.cert), 'My IP Address' (0.0.0.0), 'Peer ID Type' (IP), 'Content', 'Peer ID Type' (IP), 'Content', and 'Secure Gateway Address' (0.0.0.0).
- Security Protocol:** Contains 'VPN Protocol' (ESP), 'Pre-Shared Key' (selected), 'Certificate' (radio button), 'Encryption Algorithm' (DES), 'Authentication Algorithm' (SHA1), and an 'Advanced' button.

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

The following table describes the fields in this screen.

Table 94 Edit VPN Policies

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

Table 94 Edit VPN Policies

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

Table 94 Edit VPN Policies

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

Table 94 Edit VPN Policies

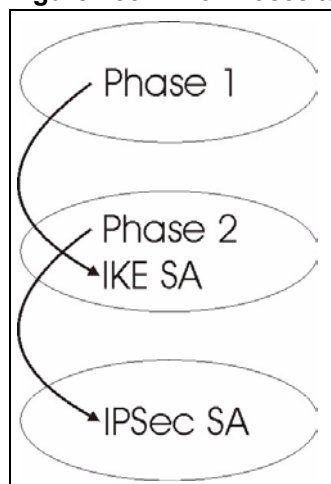
LABEL	DESCRIPTION
Peer ID Type	<p>Select IP to identify the remote IPsec router by its IP address.</p> <p>Select DNS to identify the remote IPsec router by a domain name.</p> <p>Select E-mail to identify the remote IPsec router by an e-mail address.</p>
Content	<p>The configuration of the peer content depends on the peer ID type.</p> <p>For IP, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the ZyXEL Device will use the address in the Secure Gateway Address field (refer to the Secure Gateway Address field description).</p> <p>For DNS or E-mail, type a domain name or e-mail address by which to identify the remote IPsec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.</p> <p>It is recommended that you type an IP address other than 0.0.0.0 or use the DNS or E-mail ID type in the following situations:</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 0.0.0.0 if the remote IPsec router has a dynamic WAN IP address (the Key Management field must be set to IKE).</p> <p>In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0.</p>
Security Protocol	
VPN Protocol	<p>Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below).</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>
Certificate	<p>Select the Certificate radio button to identify the ZyXEL Device by a certificate.</p> <p>Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the My Certificates screen. Click My Certificates to go to the My Certificates screen where you can view the ZyXEL Device's list of certificates.</p>

Table 94 Edit VPN Policies

LABEL	DESCRIPTION
Encryption Algorithm	<p>Select DES, 3DES, AES or NULL 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 (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. AES is faster than 3DES.</p> <p>Select NULL to set up a tunnel without encryption. When you select NULL, you do not enter an encryption key.</p>
Authentication Algorithm	<p>Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA-1 for maximum security.</p>
Advanced	Click Advanced to configure more detailed settings of your IKE key management.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.
Delete	Click Delete to delete the current rule.

16.12 IKE Phases

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

Figure 133 Two Phases to Set Up the IPsec SA

In phase 1 you must:

- Choose a negotiation mode.

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

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see [Section 16.12.3 on page 254](#). Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyXEL Device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

16.12.1 Negotiation Mode

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

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

16.12.2 Diffie-Hellman (DH) Key Groups

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

16.12.3 Perfect Forward Secrecy (PFS)

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

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

16.13 Configuring Advanced IKE Settings

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

Figure 134 Advanced VPN Policies

VPN - IKE - Advanced Setup

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

Phase 1

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

Phase 2

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

Apply Cancel

The following table describes the fields in this screen.

Table 95 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 YES from the drop-down menu to enable replay detection, or select NO to disable it.
Local Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If Local Start Port is left at 0, End will also remain at 0.
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If Remote Start Port is left at 0, End will also remain at 0.
Phase 1	

Table 95 Advanced VPN Policies

LABEL	DESCRIPTION
Negotiation Mode	Select Main or Aggressive from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Pre-Shared Key	<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 DES, 3DES or AES 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 (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. AES is faster than 3DES.</p>
Authentication Algorithm	<p>Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA-1 for maximum security.</p>
SA Life Time (Seconds)	<p>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).</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. DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.</p>
Phase 2	
Active Protocol	Use the drop-down list box to choose from ESP or AH .
Encryption Algorithm	<p>This field is available when you select ESP in the Active Protocol field.</p> <p>Select DES, 3DES, AES or NULL 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 (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. AES is faster than 3DES.</p> <p>Select NULL to set up a tunnel without encryption. When you select NULL, you do not enter an encryption key.</p>

Table 95 Advanced VPN Policies

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

16.14 Manual Key Setup

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

16.14.1 Security Parameter Index (SPI)

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

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

16.15 Configuring Manual Key

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

Figure 135 VPN: Manual Key

The screenshot shows a web-based configuration interface for a VPN. At the top, there are three tabs: 'Setup' (selected), 'Monitor', and 'VPN Global Setting'. Below the tabs, the configuration is organized into sections:

- IPSec Setup:** Includes a checkbox for 'Active', a 'Name' field (containing '2488393585'), a dropdown for 'IPSec Key Mode' (set to 'Manual'), a 'SPI' field (containing '0'), a dropdown for 'Encapsulation Mode' (set to 'Transport'), and a 'DNS Server (for IPSec VPN)' field (containing '0.0.0.0').
- Local:** Includes a dropdown for 'Local Address Type' (set to 'Range'), and two empty input fields for 'IP Address Start' and 'End / Subnet Mask'.
- Remote:** Includes a dropdown for 'Remote Address Type' (set to 'Range'), and two empty input fields for 'IP Address Start' and 'End / Subnet Mask'.
- Address Information:** Includes two empty input fields for 'My IP Address' and 'Secure Gateway Address'.
- Security Protocol:** Includes dropdowns for 'IPSec Protocol' (set to 'ESP'), 'Encryption Algorithm' (set to 'DES'), and 'Authentication Algorithm' (set to 'SHA1'). It also has two empty input fields for 'Encapsulation Key' and 'Authentication Key'.

At the bottom of the screen, there are three buttons: '<Back', 'Apply', and 'Reset'.

The following table describes the fields in this screen.

Table 96 VPN: Manual Key

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

Table 96 VPN: Manual Key (continued)

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

Table 96 VPN: Manual Key (continued)

LABEL	DESCRIPTION
My IP Address	<p>Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>The following applies if this field is configured as 0.0.0.0: The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel.</p> <p>If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.</p>
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Security Protocol	
IPSec Protocol	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH . If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described next).
Encryption Algorithm	<p>Select DES, 3DES or NULL from the drop-down list box.</p> <p>When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. Select NULL to set up a tunnel without encryption. When you select NULL, you do not enter an encryption key.</p>
Encapsulation Key (only with ESP)	With DES , type a unique key 8 characters long. With 3DES , type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slower. Select MD5 for minimal security and SHA-1 for maximum security.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for MD5 authentication or 20 characters for SHA-1 authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.

16.16 Viewing SA Monitor

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

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

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See [Section 16.6 on page 243](#) on keep alive to have the ZyXEL Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 136 VPN: SA Monitor



The following table describes the fields in this screen.

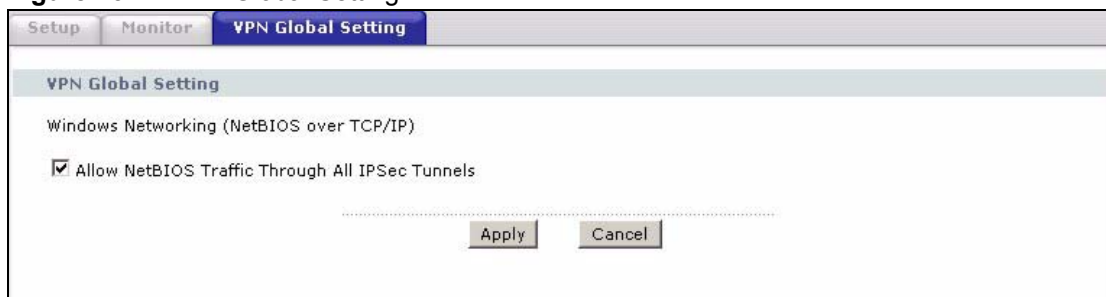
Table 97 VPN: SA Monitor

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

16.17 Configuring Global Setting

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

Figure 137 VPN: Global Setting



The following table describes the fields in this screen.

Table 98 VPN: Global Setting

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

16.18 Telecommuter VPN/IPSec Examples

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

16.18.1 Telecommuters Sharing One VPN Rule Example

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

Figure 138 Telecommuters Sharing One VPN Rule Example

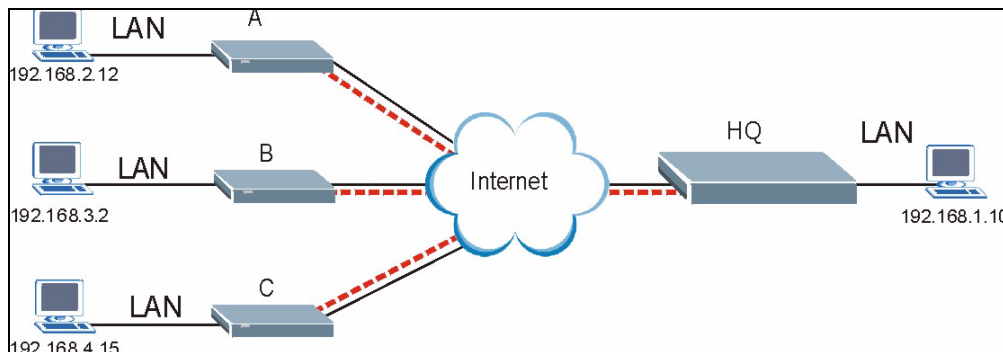


Table 99 Telecommuters Sharing One VPN Rule Example

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)

16.18.2 Telecommuters Using Unique VPN Rules Example

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

With aggressive negotiation mode (see [Section 16.12.1 on page 253](#)), 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.

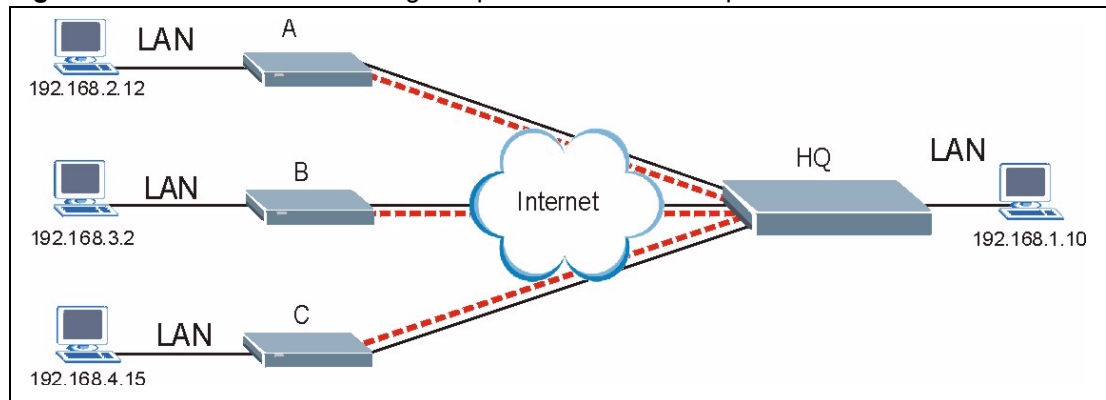
Figure 139 Telecommuters Using Unique VPN Rules Example

Table 100 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

16.19 VPN and Remote Management

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

CHAPTER 17

Certificates

This chapter gives background information about public-key certificates and explains how to use them.

17.1 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).

17.1.1 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.

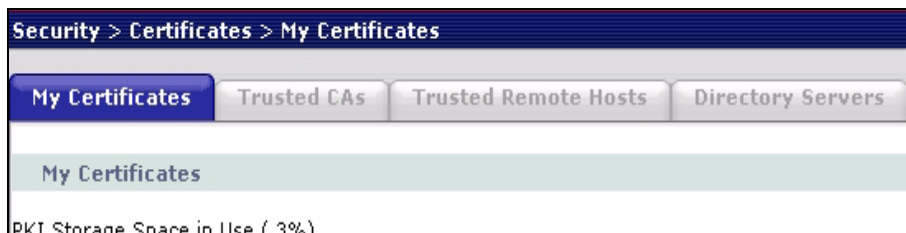
17.2 Self-signed Certificates

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.

17.3 Configuration Summary

This section summarizes how to manage certificates on the ZyXEL Device.

Figure 140 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.

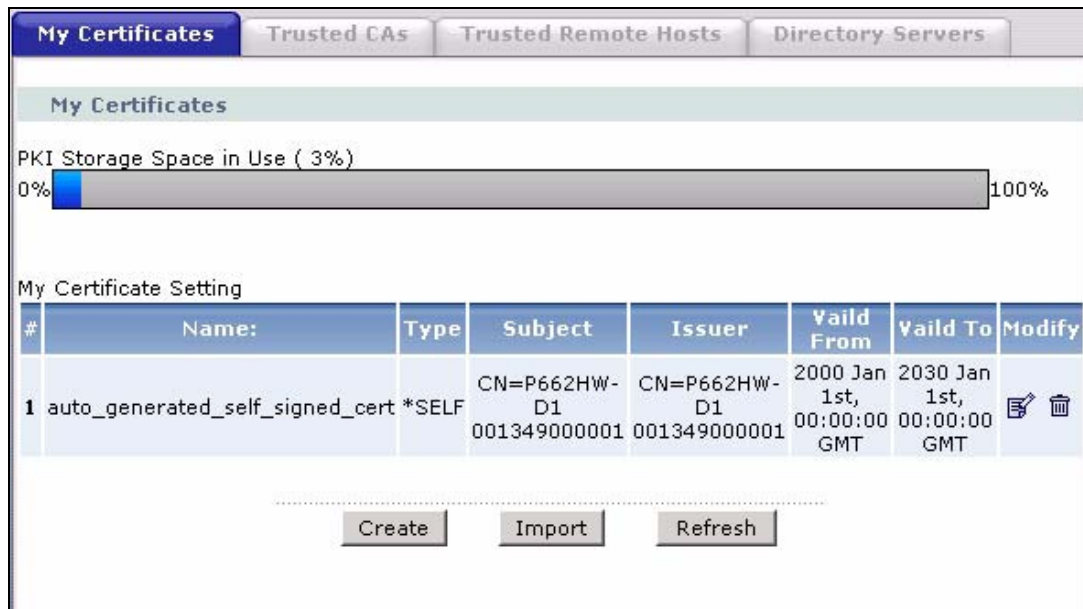
Use the **Trusted Remote Hosts** screens to import self-signed certificates.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

17.4 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 141 My Certificates



The following table describes the labels in this screen.

Table 101 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.
#	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.

Table 101 My Certificates (continued)

LABEL	DESCRIPTION
Type	<p>This field displays what kind of certificate this is.</p> <p>REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request.</p> <p>SELF represents a self-signed certificate.</p> <p>*SELF represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates.</p> <p>CERT represents a certificate issued by a certification authority.</p>
Subject	<p>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.</p>
Issuer	<p>This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.</p>
Valid From	<p>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.</p>
Valid To	<p>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.</p>
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 *SELF in the Type field.</p> <ol style="list-style-type: none"> 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the *SELF certificate. 2. Click the details icon next to another self-signed certificate (see the description on the Create button if you need to create a self-signed certificate). 3. Select the Default self-signed certificate which signs the imported remote host certificates check box. 4. Click Apply to save the changes and return to the My Certificates screen. 5. The certificate that originally showed *SELF displays SELF and you can delete it now. <p>Note that subsequent certificates move up by one when you take this action</p>
Import	<p>Click Import 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.</p>
Create	<p>Click Create to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.</p>
Refresh	<p>Click Refresh to display the current validity status of the certificates.</p>

17.5 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.

17.5.1 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 PKS#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 142 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 102 My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the ZyXEL Device.
Cancel	Click Cancel to quit and return to the My Certificates screen.

17.6 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 143 My Certificate Create

Certificates - My Certificates - 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 Trusted CAs)"/>

Request Authentication Key

.....

The following table describes the labels in this screen.

Table 103 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 Common Name is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
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 Create a self-signed certificate 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 Create a certification request and save it locally for later manual enrollment to have the ZyXEL Device generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the My Certificate Details screen (see Section 17.7 on page 272) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select Create a certification request and enroll for a certificate immediately online to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the Trusted CAs screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the Reference Number and Key if the certification authority requires them.

Table 103 My Certificate Create (continued)

LABEL	DESCRIPTION
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. Certificate Management Protocol (CMP) is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the CA Certificate drop-down list box. You must have the certification authority's certificate already imported in the Trusted CAs screen. Click Trusted CAs to go to the Trusted CAs screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication	When you select Create a certification request and enroll for a certificate immediately online , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just fill in the Key field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.
Apply	Click Apply to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates 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.

17.7 My Certificate Details

Click **Security > Certificates > My Certificates** to open the **My Certificates** screen (see [Figure 141 on page 267](#)). 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.

Figure 144 My Certificate Details

Certificates - My Certificates - Details

Certificate Name

Property

Default self-signed certificate which signs the imported remote host certificates.

Certificate Path

Searching...

Certificate Informations

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946687231
Subject	CN=P662HW-D1 001349000001
Issuer	CN=P662HW-D1 001349000001
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=001349000001@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	73:2d:72:ae:bb:90:55:7a:59:ae:39:b2:1f:09:c1:0b
SHA1 Fingerprint	32:46:e1:18:61:47:0c:8b:da:4e:2c:1a:44:50:94:1d:a6:bc:09:cf

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN CERTIFICATE-----
MIIBhTCCAS+gAwIBAgIEOG1M/zANBgkqhkiG9w0BAQUFADAiMSAwHgYDVQOExdQ
NjYySFctRDEgIDAwMTMOOTAwMDAwMTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEw
MDAwMDBaMCIXIDAEBgNVBAMTF1A2NjJIVy1EMSAgMDAxMzQ5MDAwMDAxMFwwDQYJ
KoZIhvcNAQEBBQADSwAwSAJBABK2AsjRsfw3Eok6IQL3rG2P+/MOqpWukomFnB5
X7nLrI4k6Bnq18mILg4b5rxBh/OOyJKiOEJVJSJ8JGm/PeOCwEAAANMMEswDgYD
VROPAQEABAQDAgKkMCUGA1UdEQQeMByBGjAwMTMOOTAwMDAwMUBhdXRvLmdlb5j
ZXJOMBIGA1UdEwEBAAQIMAYBAf8CAQEWdQYJKoZIhvcNAQEFBQADQQBcmg/f5dHQ
jLkoBBkhlmfEQB51ld08w2+I3gsufnomEUHbMye6XDK1LV6wI3FkkLb5isJuhT/
o/zpeIY1ypo6
```

The following table describes the labels in this screen.

Table 104 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 Refresh 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 Refresh 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 Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

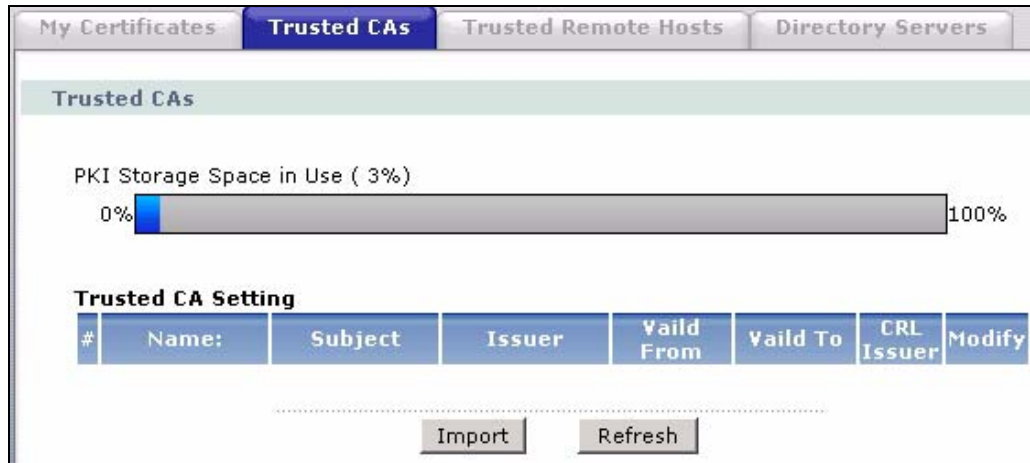
Table 104 My Certificate Details (continued)

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	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 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. 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).
Export	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Apply	Click Apply 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 Cancel to quit and return to the My Certificates screen.

17.8 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 145 Trusted CAs



The following table describes the labels in this screen.

Table 105 Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the Issues certificate revocation lists (CRL) check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Modify	Click 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 105 Trusted CAs (continued)

LABEL	DESCRIPTION
Import	Click Import 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.

17.9 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 146 Trusted CA Import

The following table describes the labels in this screen.

Table 106 Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the ZyXEL Device.
Cancel	Click Cancel to quit and return to the Trusted CAs screen.

17.10 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 147 Trusted CA Details

Certificates - Trusted CAs - Details

Certificate Name

Property

Issues certificate revocation lists (CRL)

Certificate Path

Searching...

Certificate Informations

Type	CA-signed X.509 Certificate
Version	V3
Serial Number	-78778323959442690871700631440406797776
Subject	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Issuer	CN=Root SGC Authority
Signature Algorithm	rsa-pkcs1-md5
Valid From	1999 Aug 20th, 00:30:01 GMT
Valid To	2014 Jan 28th, 07:00:00 GMT
Key Algorithm	rsaEncryption (2048 bits)
MD5 Fingerprint	6f:7e:74:a3:a1:3a:ca:bb:63:cf:74:04:17:05:fa:33
SHA1 Fingerprint	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
MTQwMTI4MDEwMDAwWjBXMQswCQYDVQQGEwJCRTEZMBcGA1UEChMQR22xvYmFsU2ln
biBudi11zYTEQMA4GA1UECzMUM9vdcBDQTEbMBkGA1UEAxMSR22xvYmFsU2lnbiBS
b290IENBMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAg7mmY3Oo+NP
in778YuDJWvqSB/xKrC51REEvfbJ0eJnZs8c3c8bSCvujYmOmQ8pgGWr6cctEsur
HEXwB6E9CjDNFY1P+N3UjFAVH09Q7sQu9/zpUvKRfeBt1TUwj15Dc/JB6dVq47KJ
O1Y5OG8GPIhpWypNxadUuGyJzJv5PMr1/Yn1EjySeJbW3HRukORhOY3HRrJ1Dobo
GYrVbWzVeBaVounICjrr8iQTT3NUkxOF0hu8HjS1iwWMuXeLsdsfIJGrCVNukM57
-----
```

The following table describes the labels in this screen.

Table 107 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 Refresh 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 Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

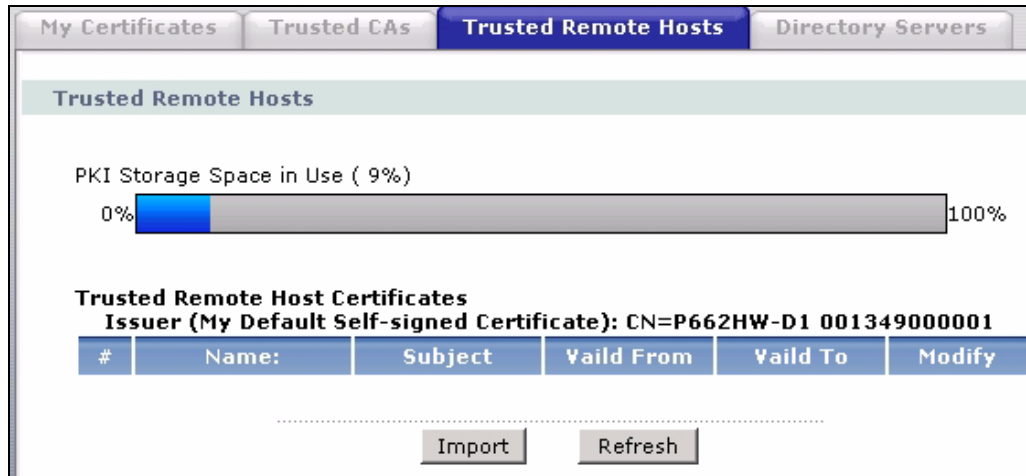
Table 107 Trusted CA Details (continued)

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 Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Apply	Click Apply 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 Cancel to quit and return to the Trusted CAs screen.

17.11 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 148 Trusted Remote Hosts

The following table describes the labels in this screen.

Table 108 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 Import 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.

17.12 Verifying a Trusted Remote Host's Certificate

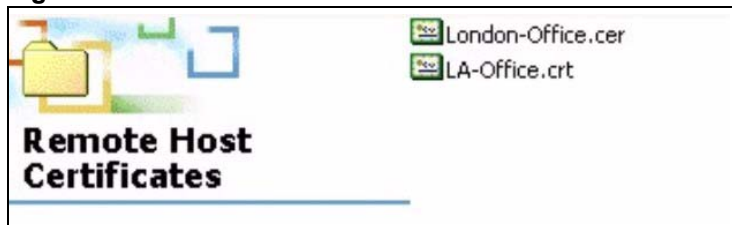
Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

17.12.1 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.

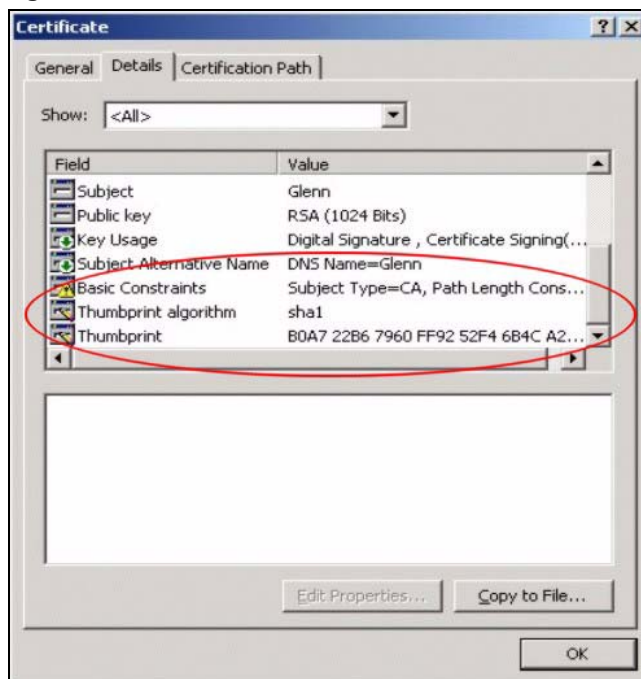
- 1 Browse to where you have the remote host's certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 149 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 150 Certificate Details



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

17.13 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 151 Trusted Remote Host Import

Certificates - Trusted Remote Hosts - Import

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

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

File Path:

.....

The following table describes the labels in this screen.

Table 109 Trusted Remote Host Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the ZyXEL Device.
Cancel	Click Cancel to quit and return to the Trusted Remote Hosts screen.

17.14 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 152 Trusted Remote Host Details

Certificates - Trusted Remote Hosts - Details

Certificate Name

Certificate Path
 Refresh

Certificate Path

Type	CA-signed X.509 Certificate
Version	V3
Serial Number	144494120486291136762321733029693522805
Subject	CN=ZyZEL
Issuer	CN=P662HW-D1 001349000001
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2005 Sep 2nd, 02:46:18 GMT (Not Yet Valid!)
Valid To	2010 Sep 2nd, 02:54:46 GMT
Key Algorithm	rsaEncryption (2048 bits)
Key Usage	DigitalSignature
Basic Constraint	Path Length Constraint=10
CRL Distribution Points	[1]CRL Distribution Point
MD5 Fingerprint	Full Name: URI=http://zyxel-g97zfcjk2/CertEnroll/ZyZEL.crl, URI=
SHA1 Fingerprint	eb:be:19:67:f5:81:ff:be:85:63:66:ff:6d:5b:8a:b7 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
MSAwHgYDVQQDExdQNjYySFctRDEgIDAuMTMOOTAwMDAwMTAeFw0wNTA5MDIwMjQ2
MThaFw0xMDA5MDIwMjU0NDZaMBAxDjAMBGNVBAMTBVp5WkVMMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxKO4T3OpQHIVMits15IrupkZ1fSgg9KR2/tW
FogGTWJ6JVMhuqSybaxTORfd07LqBnLiFP12UZxlrNVvfnPzGwf/Yvj1FPfu03Nq
Y/6zkySeZSt9HR1zWJ6uC6hwJURpSxZizGvD4E1Ju609VKyhdnX7aCODaNS2p8WD
Tc+p+YFhqDVCmOKRNmKjQBPgRsMbzxrd0AYRL3ZHe/lmvOdIVZNATVMmHC2Vx9I/
I3O96TIVcUdNI5d93idwxTFhDGB+ogMFGx9nu2XCQL4yuOGntfFmYR3/3icH75r+
tHD3yFacTF1fAojo8WXvc7iWxDm+UGbUg9/U+jKL6Y1PSjxihQIDAQABo4HCMIG/
    
```

The following table describes the labels in this screen.

Table 110 Trusted Remote Host Details

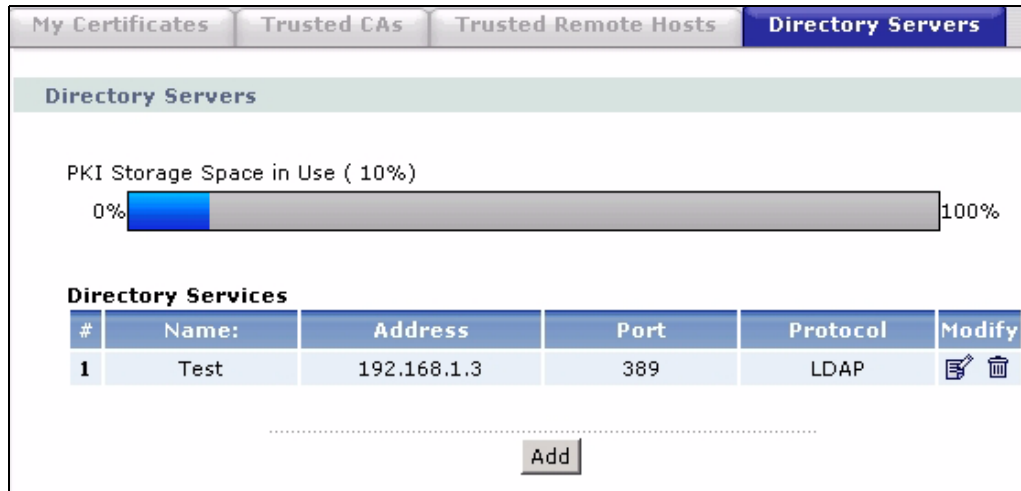
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click the Refresh button to have this read-only text box 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 Refresh 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 110 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 Section 17.12 on page 282 for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 17.12 on page 282 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 Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Apply	Click Apply to save your changes back to the ZyXEL Device. You can only change the name of the certificate.
Cancel	Click Cancel to quit configuring this screen and return to the Trusted Remote Hosts screen.

17.15 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 153 Directory Servers

The following table describes the labels in this screen.

Table 111 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 Add to open a screen where you can configure information about a directory server so that the ZyXEL Device can access it.

17.16 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 154 Directory Server Add

The following table describes the labels in this screen.

Table 112 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. LDAP (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates. ¹
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.
Server Port	This field displays the default server port number of the protocol that you select in the Access Protocol field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The ZyXEL Device may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to quit configuring this screen and return to the Directory Servers screen.

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

CHAPTER 18

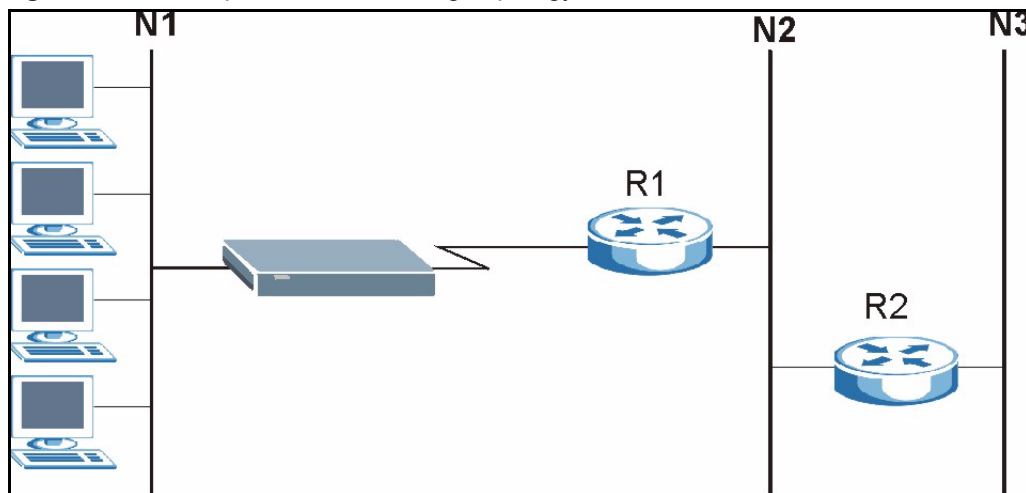
Static Route

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

18.1 Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

Figure 155 Example of Static Routing Topology



18.2 Configuring Static Route

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

Figure 156 Static Route

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

The following table describes the labels in this screen.

Table 113 Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field shows whether this static route is active (Yes) or not (No).
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the Delete icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.

18.2.1 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 157 Static Route Edit

The screenshot shows a web-based configuration interface for a static route. The title is "Static Route Setup". It includes a checkbox for "Active". Below are four input fields: "Route Name" (empty), "Destination IP Address" (0.0.0.0), "IP Subnet Mask" (0.0.0.0), and "Gateway IP Address" (0.0.0.0). At the bottom, there are three buttons: "Back", "Apply", and "Cancel".

The following table describes the labels in this screen.

Table 114 Static Route Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 19

Bandwidth Management

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

19.1 Bandwidth Management Overview

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

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

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

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 any interface must be less than or equal to the speed allocated to that interface in the **Bandwidth Management Summary** screen.

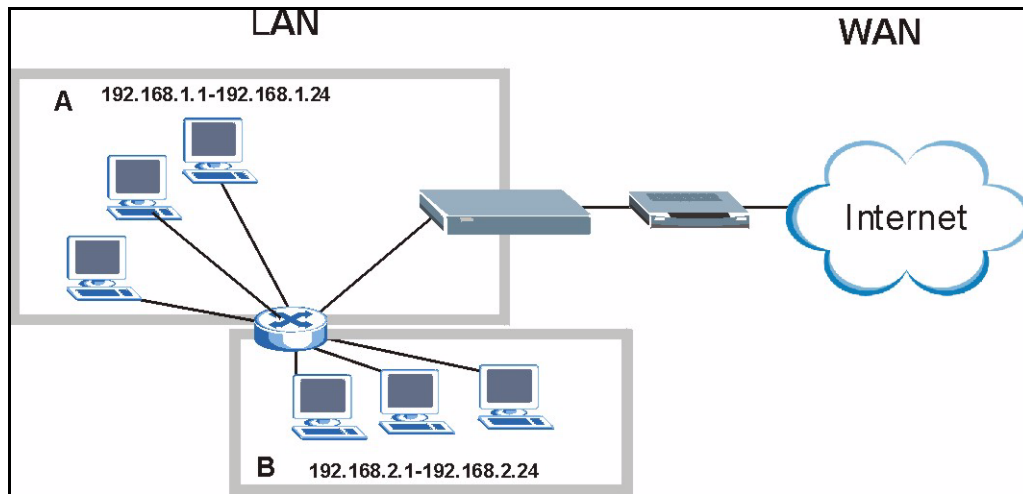
19.2 Application-based Bandwidth Management

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

19.3 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

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

Figure 158 Subnet-based Bandwidth Management Example

19.4 Application and Subnet-based Bandwidth Management

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

Table 115 Application and Subnet-based Bandwidth Management Example

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

19.5 Scheduler

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

19.5.1 Priority-based Scheduler

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

19.5.2 Fairness-based Scheduler

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

19.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see [Figure 159 on page 298](#)) 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.

19.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

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

- 1 Leave some of the interface's bandwidth unbudgeted.
- 2 Do not enable the interface's **Maximize Bandwidth Usage** option.
- 3 Do not enable bandwidth borrowing on the child-classes that have the root class as their parent (see [Section 19.8 on page 299](#)).

19.6.2 Maximize Bandwidth Usage Example

Here is an example of a ZyXEL Device that has maximize bandwidth usage enabled on an interface. The following table shows each bandwidth class's bandwidth budget. The classes are set up based on subnets. The interface is set to 10240 kbps. Each subnet is allocated 2048 kbps. The 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 116 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.

19.6.2.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth

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

Table 117 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

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

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

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

- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

19.6.2.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth

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

Table 118 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

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

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

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

19.6.3 Bandwidth Management Priorities

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

Table 119 Bandwidth Management Priorities

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

19.7 Configuring Summary

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

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

Figure 159 Bandwidth Management: Summary

Summary Rule Setup Monitor

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 Reset

The following table describes the labels in this screen.

Table 120 Media Bandwidth Management: Summary

LABEL	DESCRIPTION
Interface	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class. The recommendation is to set this speed to match what the interface's connection can handle. For example, set the WAN interface speed to 10000 kbps if the DSL connection has an upstream speed of 10Mbps.
Scheduler	Select either Priority-Based or Fairness-Based from the drop-down menu to control the traffic flow. Select Priority-Based to give preference to bandwidth classes with higher priorities. Select Fairness-Based to treat all bandwidth classes equally.
Max Bandwidth Usage	Select this check box to have the ZyXEL Device divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the speed of this interface (see the Speed field description).
Apply	Click Apply to save your settings back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

19.8 Bandwidth Management Rule Setup

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

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

Figure 160 Bandwidth Management: Rule Setup

The following table describes the labels in this screen.

Table 121 Bandwidth Management: Rule Setup

LABEL	DESCRIPTION
Direction	Select the direction of traffic to which you want to apply bandwidth management.
Service	Select a service for your rule or you can select User Defined to go to the screen where you can define your own.
Priority	Select a priority from the drop down list box. Choose High , Mid or Low .
Bandwidtht (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.
Add	Click this button to add a rule to 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.
Bandwidtht (kbps)	This is the maximum bandwidth allowed for the rule in kbps.

Table 121 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 Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

19.8.1 Rule Configuration

Click the Edit icon or select **User Defined** from the **Service** drop-down list in the **Rule Setup** screen 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 161 Bandwidth Management Rule Configuration

Rule Configuration

Active

Rule Name:

BW Budget: (Kbps)

Priority:

Use All Managed Bandwidth

Filter Configuration

Service:

Destination Address:

Destination Subnet Netmask:

Destination Port:

Source Address:

Source Subnet Netmask:

Source Port:

Protocol:

Back Apply Cancel

The following table describes the labels in this screen.

Table 122 Bandwidth Management Rule Configuration

LABEL	DESCRIPTION
Rule Configuration	
Active	<p>Select this check box to have the ZyXEL Device apply this bandwidth management rule.</p> <p>Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule.</p> <p>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.</p>
Rule Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
BW Budget	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule.
Priority	Select a priority from the drop down list box. Choose High , Mid or Low .
Use All Managed Bandwidth	<p>Select this option to allow a rule to borrow unused bandwidth on the interface.</p> <p>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.</p>
Filter Configuration	
Service	<p>This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).</p> <p>SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select SIP from the drop-down list box to configure this bandwidth filter for traffic that uses SIP.</p> <p>File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select FTP from the drop-down list box to configure this bandwidth filter for FTP traffic.</p> <p>H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Select H.323 from the drop-down list box to configure this bandwidth filter for traffic that uses H.323.</p> <p>Select User defined from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select User defined, you need to configure at least one of the following fields (other than the Subnet Mask fields which you only enter if you also enter a corresponding destination or source IP address).</p>
Destination Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a Destination Address . Refer to the appendices for more information on IP subnetting.

Table 122 Bandwidth Management Rule Configuration (continued)

LABEL	DESCRIPTION
Destination Port	Enter the port number of the destination. See Table 123 on page 302 for some common services and port numbers. A blank destination IP address means any destination IP address.
Source Address	Enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Source Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a Source Address . Refer to the appendices for more information on IP subnetting. A blank source port means any source port number.
Source Port	Enter the port number of the source. See Table 123 on page 302 for some common services and port numbers.
Protocol	Select the protocol (TCP or UDP) or select User defined and enter the protocol (service type) number. ID "0" means any protocol number.
Back	Click Back to go to the previous screen.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

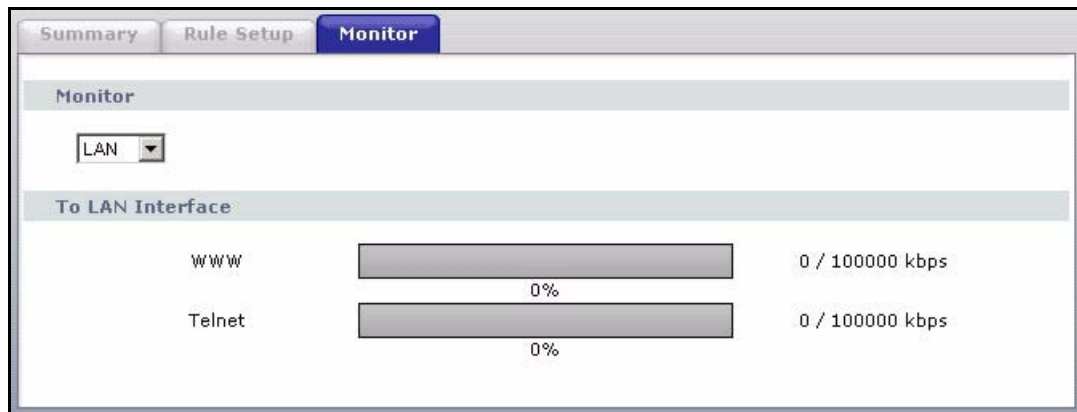
The following table describes common services with their associated port numbers.

Table 123 Services and Port Numbers

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

19.9 Bandwidth Monitor

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

Figure 162 Bandwidth Management: Monitor

CHAPTER 20

Dynamic DNS Setup

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

20.1 Dynamic DNS Overview

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

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

20.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

See [Section 20.2 on page 305](#) for configuration instruction.

20.2 Configuring Dynamic DNS

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

See [Section 20.1 on page 305](#) for more information.

Figure 163 Dynamic DNS

The following table describes the fields in this screen.

Table 124 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 Custom DNS is selected in the DDNS Type field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.

Table 124 Dynamic DNS (continued)

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP Address	<p>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.</p> <p>Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.</p>
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 21

Remote Management Configuration

This chapter provides information on configuring remote management.

21.1 Remote Management Overview

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

Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

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

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

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

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

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

- 1 Telnet
- 2 HTTP

21.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

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

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

21.1.2 Remote Management and NAT

When NAT is enabled:

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

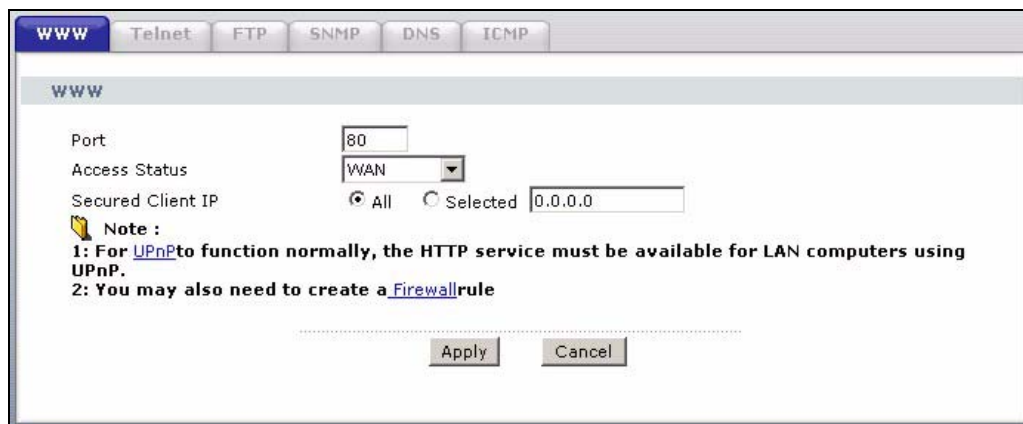
21.1.3 System Timeout

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

21.2 WWW

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

Figure 164 Remote Management: WWW



The screenshot shows the 'WWW' configuration page. At the top, there are tabs for 'WWW', 'Telnet', 'FTP', 'SNMP', 'DNS', and 'ICMP'. The 'WWW' tab is selected. Below the tabs, the 'WWW' title is displayed. The configuration fields are as follows:

- Port:** A text input field containing the value '80'.
- Access Status:** A dropdown menu with 'WAN' selected.
- Secured Client IP:** Radio buttons for 'All' (selected) and 'Selected', followed by a text input field containing '0.0.0.0'.

Below the configuration fields, there is a **Note** section with two points:

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

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

The following table describes the labels in this screen.

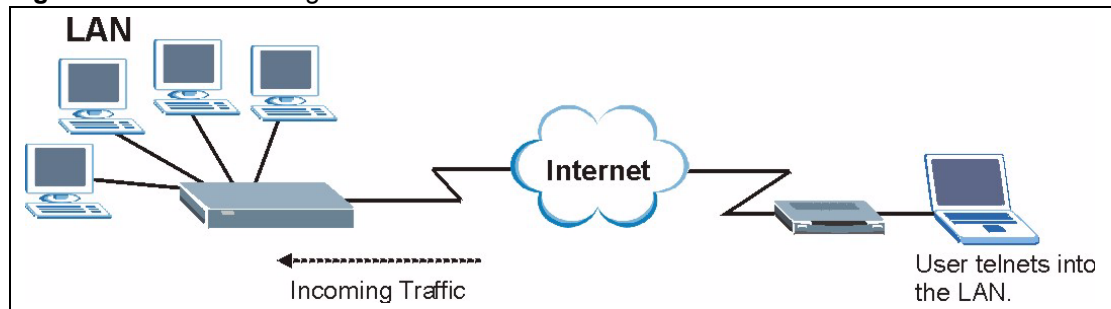
Table 125 Remote Management: WWW

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

21.3 Telnet

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

Figure 165 Telnet Configuration on a TCP/IP Network



21.4 Configuring Telnet

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

Figure 166 Remote Management: Telnet

The following table describes the labels in this screen.

Table 126 Remote Management: Telnet

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

21.5 Configuring FTP

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

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

Figure 167 Remote Management: FTP

The following table describes the labels in this screen.

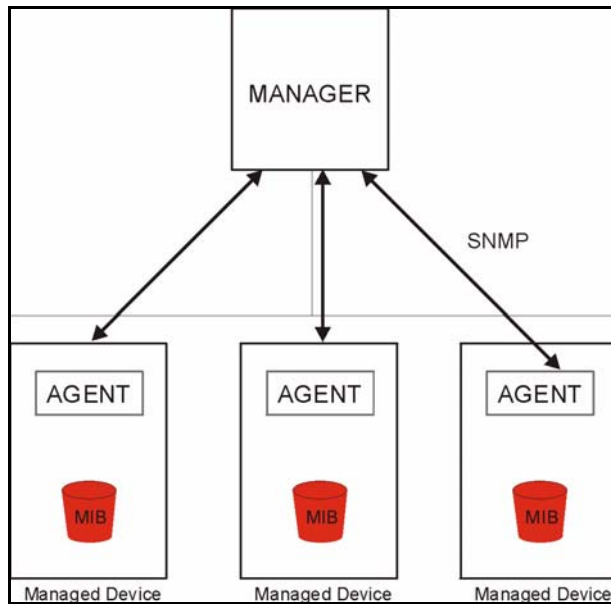
Table 127 Remote Management: FTP

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

21.6 SNMP

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

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

Figure 168 SNMP Management Model

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

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

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

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

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

21.6.1 Supported MIBs

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

21.6.2 SNMP Traps

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

Table 128 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).
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.

21.6.3 Configuring SNMP

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

Figure 169 Remote Management: SNMP

The following table describes the labels in this screen.

Table 129 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select All to allow any computer to access the ZyXEL Device using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

21.7 Configuring DNS

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

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

Figure 170 Remote Management: DNS

The following table describes the labels in this screen.

Table 130 Remote Management: DNS

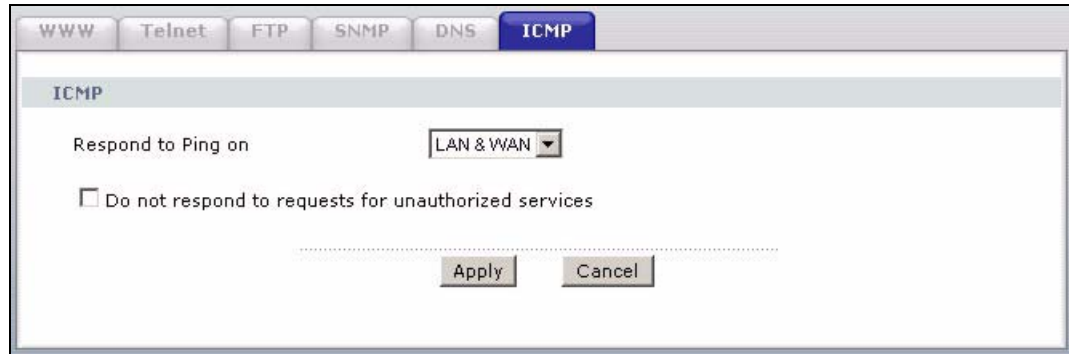
LABEL	DESCRIPTION
Port	The DNS service port number is 53 and cannot be changed here.
Access Status	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP	A secured client is a "trusted" computer that is allowed to send DNS queries to the ZyXEL Device.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

21.8 Configuring ICMP

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

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

Figure 171 Remote Management: ICMP



The following table describes the labels in this screen.

Table 131 Remote Management: ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN & WAN to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. By default this option is not selected and the ZyXEL Device will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the ZyXEL Device's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyXEL Device reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

21.9 TR-069

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

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

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

Note: In this example **a.b.c.d** is the IP address of CNM Access. You must change this value to reflect your actual management server IP address or domain name. See [Table 132 on page 319](#) for detailed descriptions of the commands.

Figure 172 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 132 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 132 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 22

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

22.1 Introducing Universal Plug and Play

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

See [Section 22.2.1 on page 322](#) for configuration instructions.

22.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

22.1.2 NAT Traversal

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

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

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

See the NAT chapter for more information on NAT.

22.1.3 Cautions with UPnP

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

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.

22.2 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.

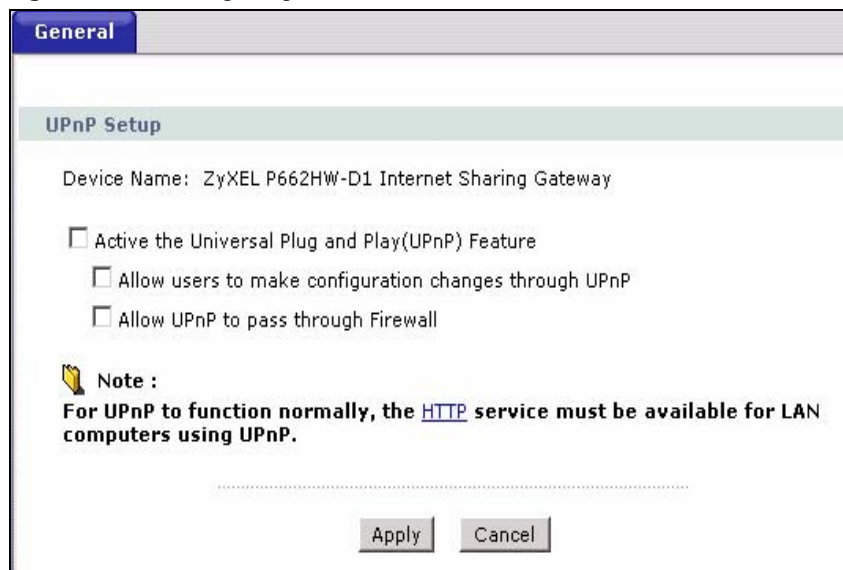
See the following sections for examples of installing and using UPnP.

22.2.1 Configuring UPnP

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

See [Section 22.1 on page 321](#) for more information.

Figure 173 Configuring UPnP



The screenshot shows a web-based configuration window titled "UPnP Setup" under a "General" tab. The window displays the following information:

- Device Name: ZyXEL P662HW-D1 Internet Sharing Gateway
- Three unchecked checkboxes:
 - Active the Universal Plug and Play(UPnP) Feature
 - Allow users to make configuration changes through UPnP
 - Allow UPnP to pass through Firewall
- A **Note** icon 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 133 Configuring UPnP

LABEL	DESCRIPTION
Active the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click Apply to save the setting to the ZyXEL Device.
Cancel	Click Cancel to return to the previously saved settings.

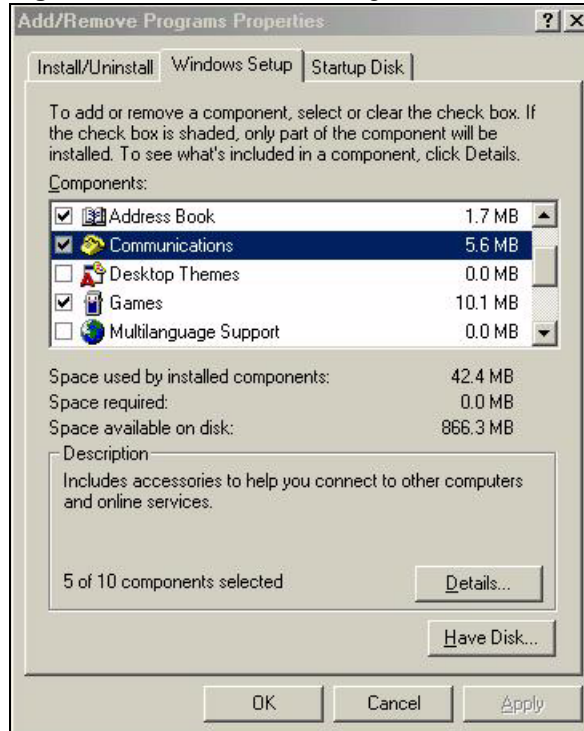
22.3 Installing UPnP in Windows Example

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

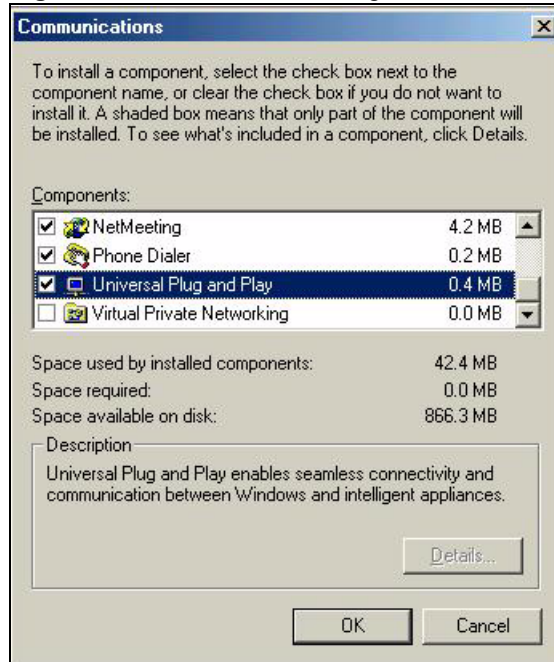
Installing UPnP in Windows Me

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

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

Figure 174 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 175 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.

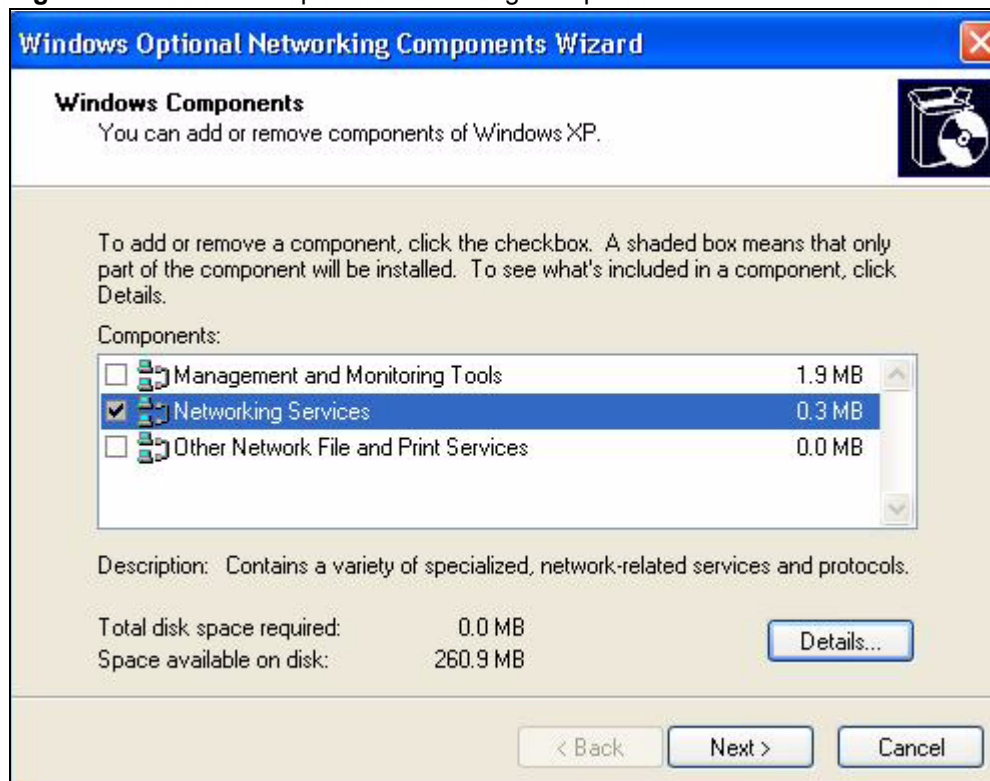
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components**

Figure 176 Network Connections

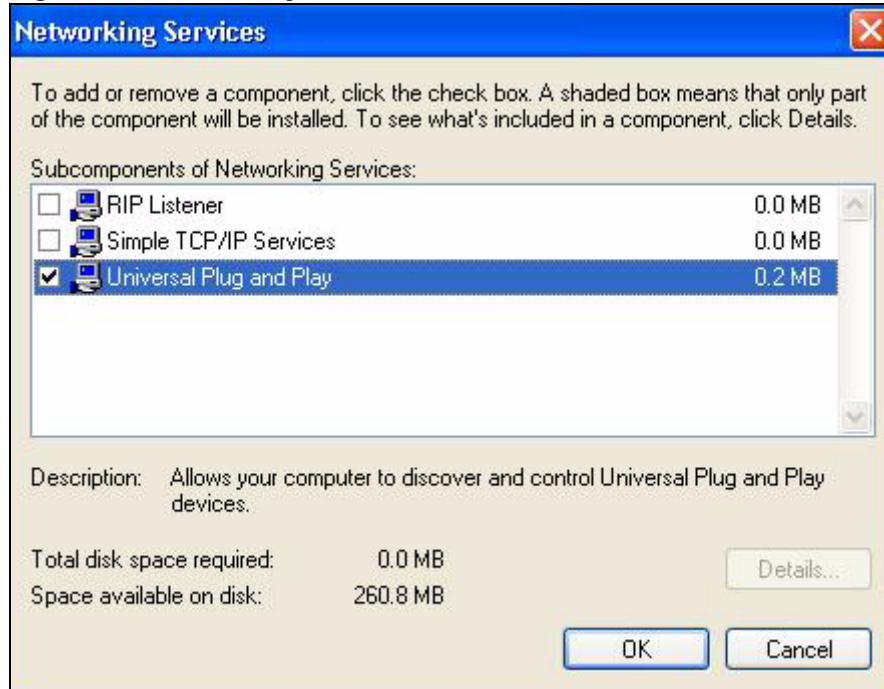


- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 177 Windows Optional Networking Components Wizard



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

Figure 178 Networking Services

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

22.4 Using UPnP in Windows XP Example

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

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

Auto-discover Your UPnP-enabled Network Device

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

Figure 179 Network Connections

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

Figure 180 Internet Connection Properties

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

Figure 181 Internet Connection Properties: Advanced Settings

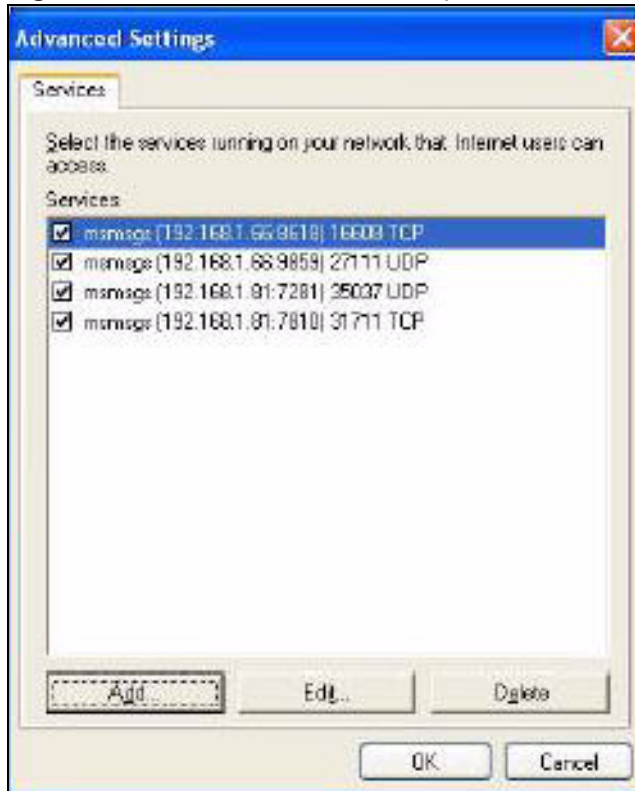
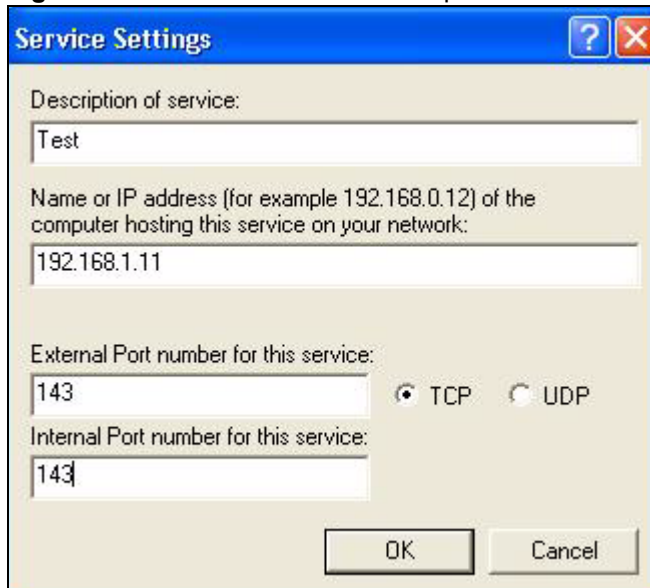


Figure 182 Internet Connection Properties: Advanced Settings: Add



- 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 183 System Tray Icon

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

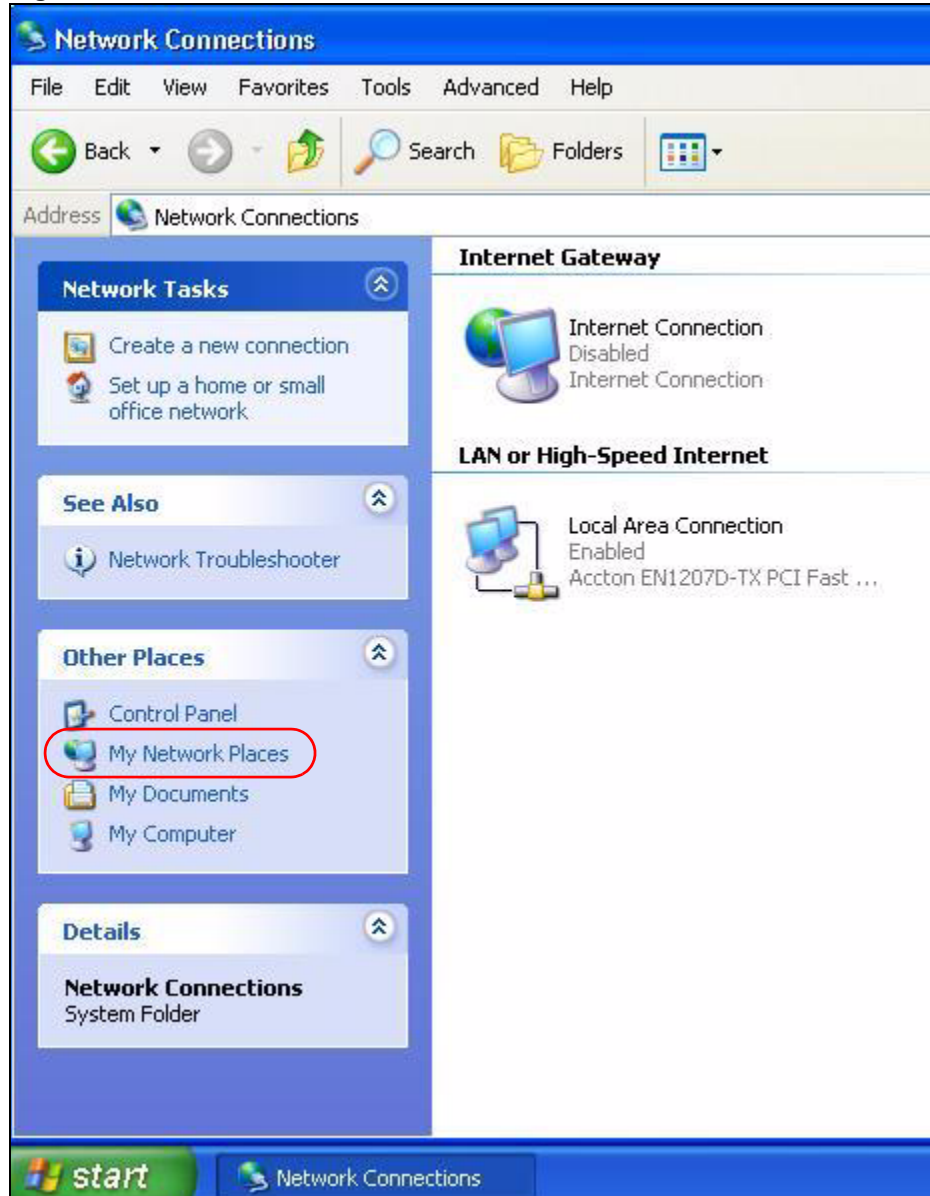
Figure 184 Internet Connection Status

Web Configurator Easy Access

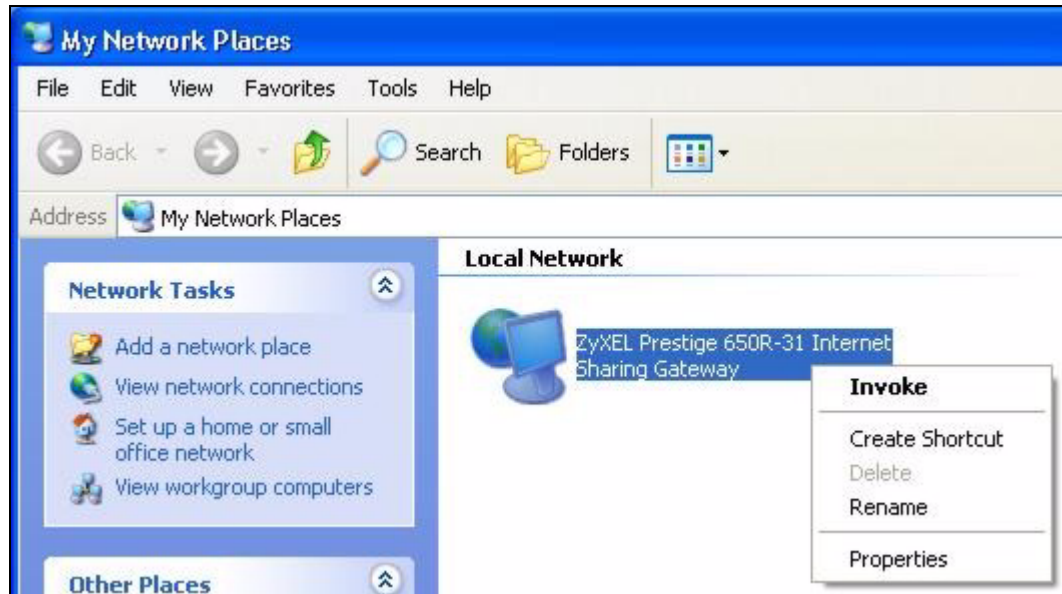
With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

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 185 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 186 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 187 Network Connections: My Network Places: Properties: Example

CHAPTER 23

System

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

23.1 General Setup

23.1.1 General Setup and System Name

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

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

23.1.2 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 188 System General Setup

The following table describes the labels in this screen.

Table 134 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 CLI (Command Line Interpreter)) 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	
User Password	If you log in with the user password you can only view the ZyXEL Device status. The default user password is user .
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.

Table 134 System General Setup

LABEL	DESCRIPTION
Admin Password	In addition to the wizard setup, if you log in with the admin password you can also view and configure the advanced features on the ZyXEL Device.
Old Password	Type the default administrator password (1234) or the existing password you use to access the system for configuring advanced features in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Cancel	Click Cancel to begin configuring this screen afresh.

23.2 Time Setting

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

Figure 189 System Time Setting

The screenshot shows the 'Time Setting' configuration page with the following details:

- Current Time and Date:**
 - Current Time: 00:36:06
 - Current Date: 2000-01-01
- Time and Date Setup:**
 - Manual
 - New Time (hh:mm:ss): 0 : 30 : 59
 - New Date (yyyy/mm/dd): 2000 / 1 / 1
 - Get from Time Server
 - Time Protocol: Daytime (RFC-867)
 - Time Server Address: 0.0.0.0
- Time Zone Setup:**
 - Time Zone: (GMT) Greenwich Mean Time : Dublin Edinburgh, Lisbon, London
 - Enable Daylight Savings
 - Start Date: First Sunday of January (2000-01-02) at 0 o'clock
 - End Date: First Sunday of January (2000-01-02) at 0 o'clock

The following table describes the fields in this screen.

Table 135 System Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
Current Date	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set Time and Date Setup to Manual , enter the new time in this field and then click Apply .
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set Time and Date Setup to Manual , enter the new date in this field and then click Apply .
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, NTP (RFC 1305) , is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.

Table 135 System Time Setting (continued)

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

CHAPTER 24

Logs

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

24.1 Logs Overview

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

24.1.1 Alerts and Logs

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

24.2 Viewing the Logs

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 24.3 on page 340](#)).

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 190 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 136 View Log

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

24.3 Configuring Log Settings

Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device is to record. See [Section 24.1 on page 339](#) 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 191 Log Settings

The following table describes the fields in this screen.

Table 137 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 137 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"> • Daily • Weekly • Hourly • When Log is Full • None. <p>If you select Weekly or Daily, specify a time of day when the E-mail should be sent. If you select Weekly, then also specify which day of the week the E-mail should be sent. If you select When Log is Full, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click Active to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click Apply to save your customized settings and exit this screen.
Cancel	Click Cancel to return to the previously saved settings.

24.4 SMTP Error Messages

The following table lists common SMTP errors.

Table 138 SMTP Error Messages

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

24.4.1 Example E-mail Log

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

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

Figure 192 E-mail Log Example

```
Subject:
  Firewall Alert From ZyXEL Device
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 25

Tools

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

25.1 Firmware Upgrade

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "ZyXEL Device.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

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

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

Figure 193 Firmware Upgrade

The following table describes the labels in this screen.

Table 139 Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.

Table 139 Firmware Upgrade (continued)

LABEL	DESCRIPTION
Browse...	Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.

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

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

Figure 194 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 195 Network Temporarily Disconnected

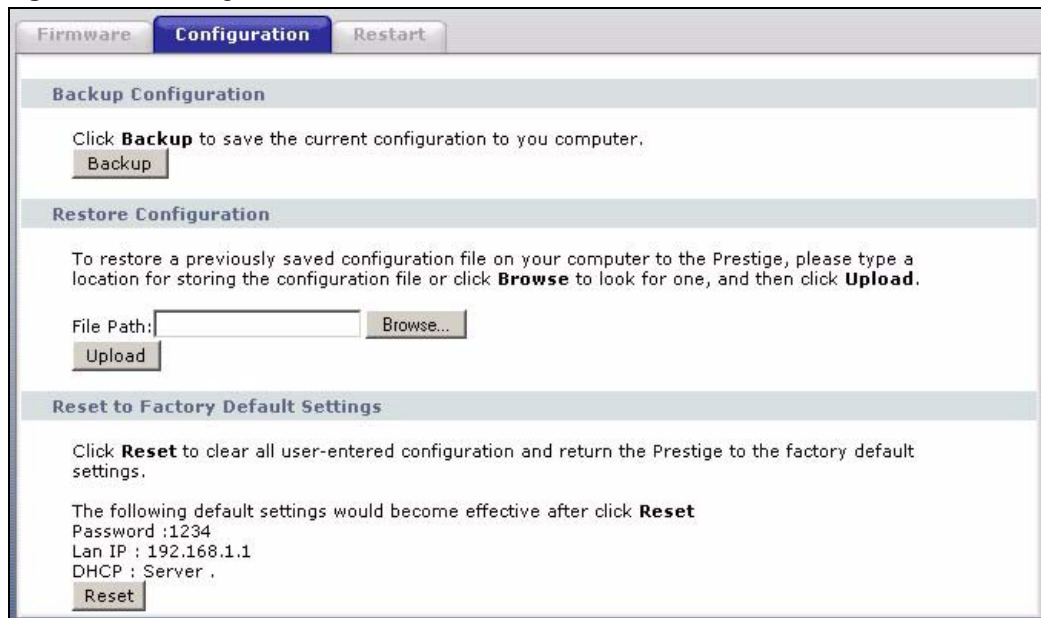
After two minutes, log in again and check your new firmware version in the **Status** screen.

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

Figure 196 Error Message

25.2 Configuration Screen

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

Figure 197 Configuration

25.2.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer

25.2.2 Restore Configuration

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

Table 140 Maintenance Restore Configuration

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

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

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

Figure 198 Configuration Restore Successful



The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 199 Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

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

Figure 200 Configuration Restore Error

25.2.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults.

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

25.3 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 201 Restart Screen

CHAPTER 26

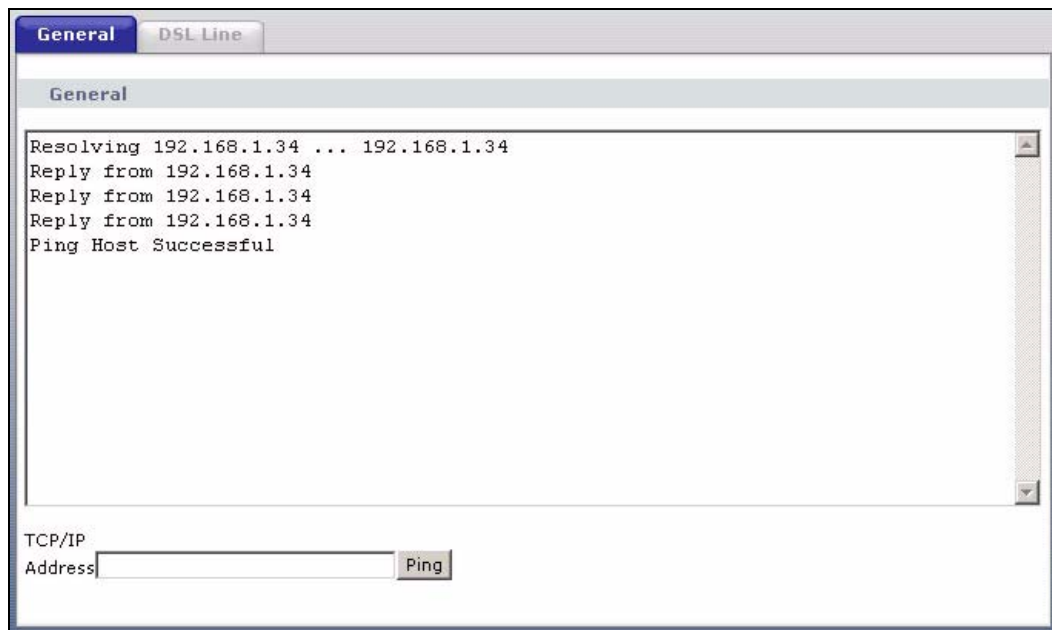
Diagnostic

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

26.1 General Diagnostic

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

Figure 202 Diagnostic: General



The following table describes the fields in this screen.

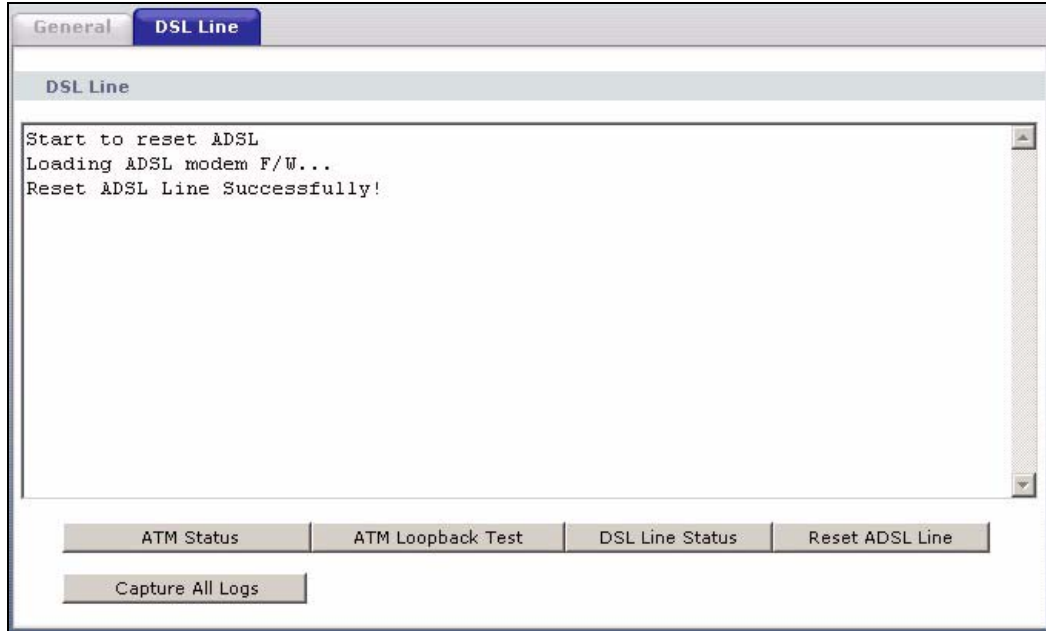
Table 141 Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.

26.2 DSL Line Diagnostic

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

Figure 203 Diagnostic: DSL Line



The following table describes the fields in this screen.

Table 142 Diagnostic: DSL Line

LABEL	DESCRIPTION
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
DSL Line Status	Click this button to view the DSL port's line operating values and line bit allocation.
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
Capture All Logs	Click this button to display all logs generated with the DSL line.

CHAPTER 27

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

27.1 Problems Starting Up the ZyXEL Device

Table 143 Troubleshooting Starting Up Your ZyXEL Device

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the ZyXEL Device.	<p>Make sure that the ZyXEL Device's power adaptor is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure that the ZyXEL Device and the power source are both turned on.</p> <p>Turn the ZyXEL Device off and on.</p> <p>If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</p>

27.2 Problems with the LAN

Table 144 Troubleshooting the LAN

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

27.3 Problems with the WAN

Table 145 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The DSL LED is off.	Check the telephone wire and connections between the ZyXEL Device DSL port and the wall jack.
	Make sure that the telephone company has checked your phone line and set it up for DSL service.
	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to the Table 142 on page 352 .
I cannot get a WAN IP address from the ISP.	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name. The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct Service Type , User Name and Password (be sure to use the correct casing). Refer to the WAN Setup chapter.
I cannot access the Internet.	Make sure the ZyXEL Device is turned on and connected to the network. Verify your WAN settings. Refer to the chapter on WAN setup. Make sure you entered the correct user name and password. If you use PPPoE pass through, make sure that bridge mode is turned on.
The Internet connection disconnects.	Check the schedule rules. If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to Chapter 5 on page 85 . Contact your ISP.

27.4 Problems Accessing the ZyXEL Device

Table 146 Troubleshooting Accessing the ZyXEL Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	<p>The default user password is "user" and admin password is "1234". The Password field is case-sensitive. Make sure that you enter the correct password using the proper case.</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 the chapter on remote management for details.</p> <p>Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p>

27.4.1 Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

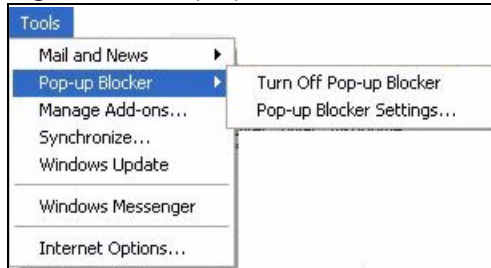
27.4.1.1 Internet Explorer Pop-up Blockers

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

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

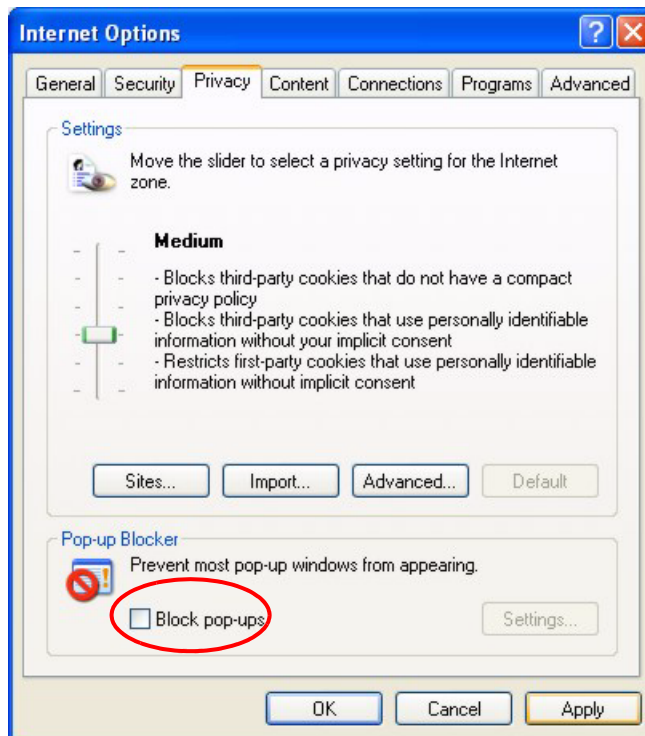
27.4.1.1.1 Disable pop-up Blockers

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

Figure 204 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.

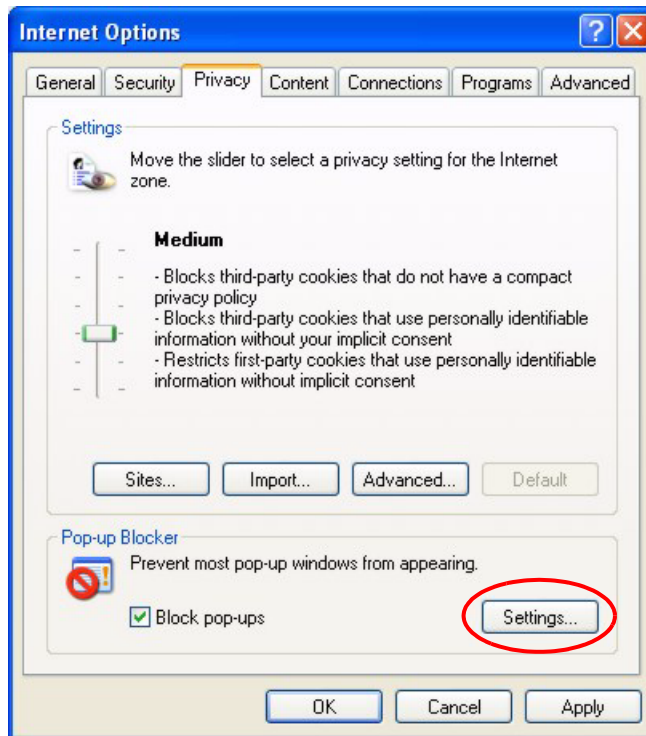
Figure 205 Internet Options

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

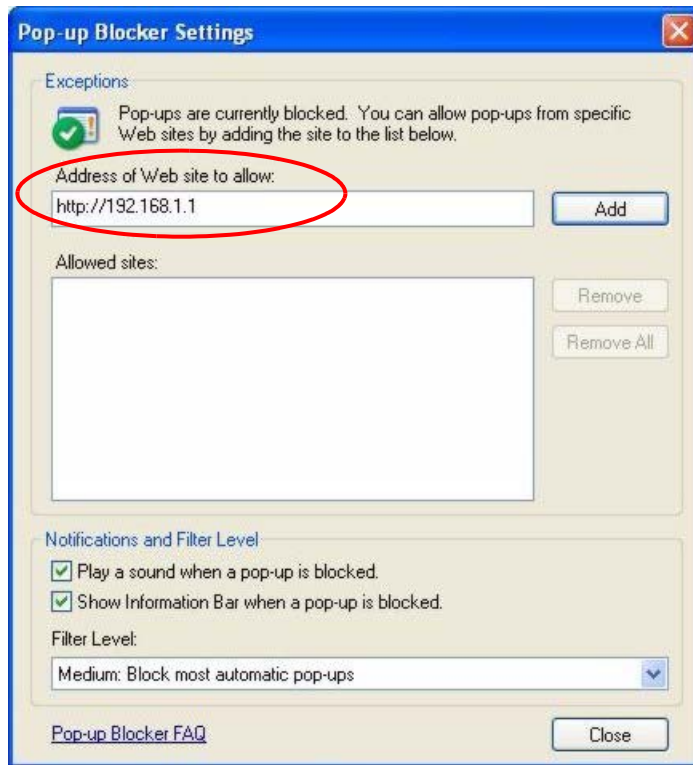
27.4.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 206 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 207 Pop-up Blocker Settings

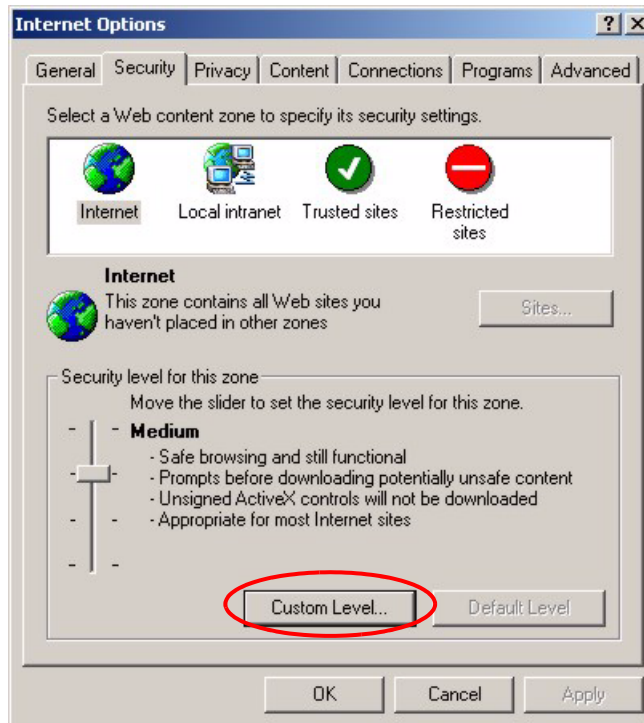
5 Click **Close** to return to the **Privacy** screen.

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

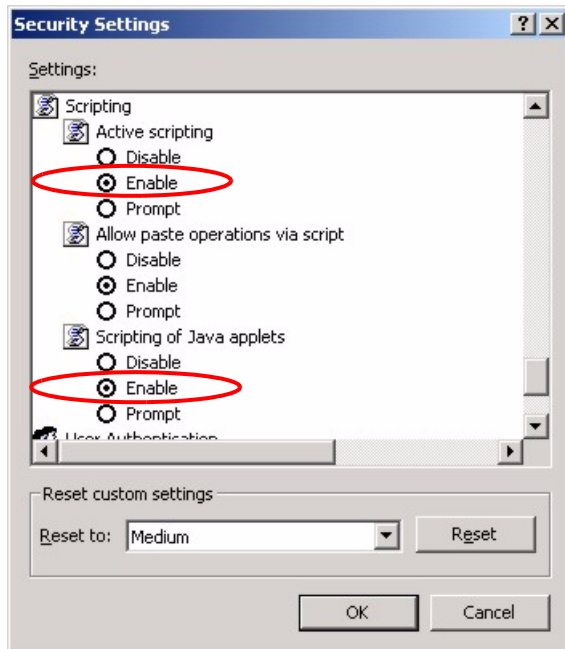
27.4.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

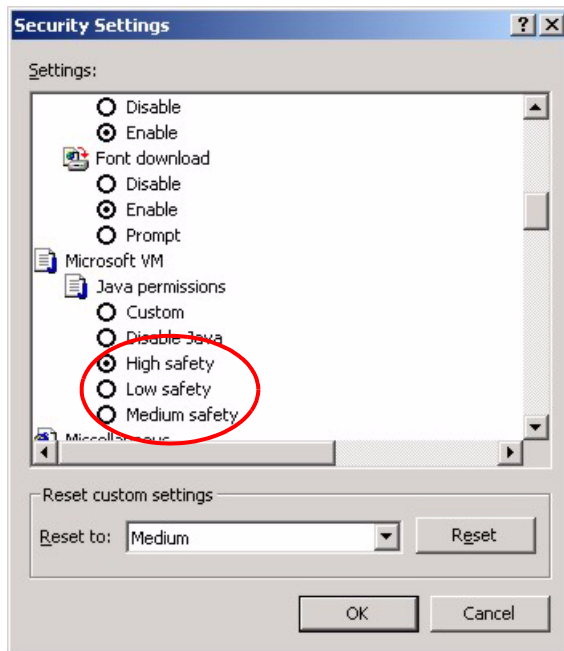
Figure 208 Internet Options

- 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 209 Security Settings - Java Scripting

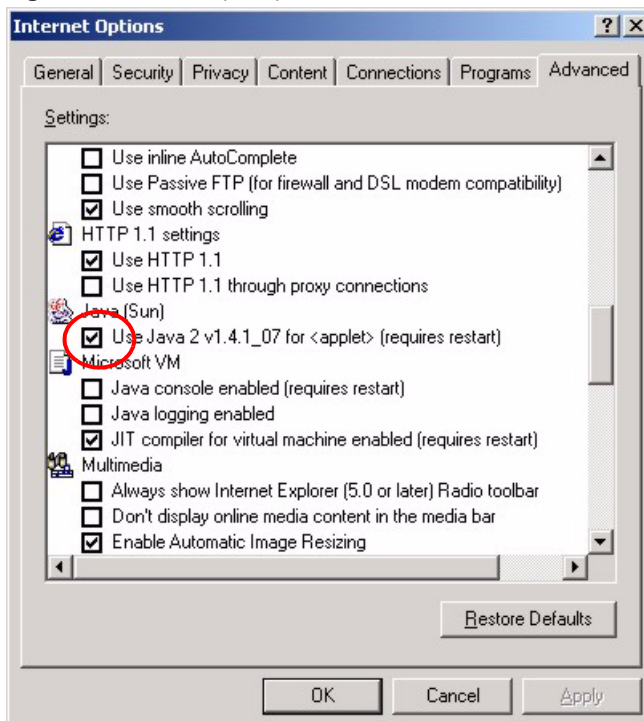
27.4.1.3 Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 210 Security Settings - Java

27.4.1.3.1 JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 211 Java (Sun)

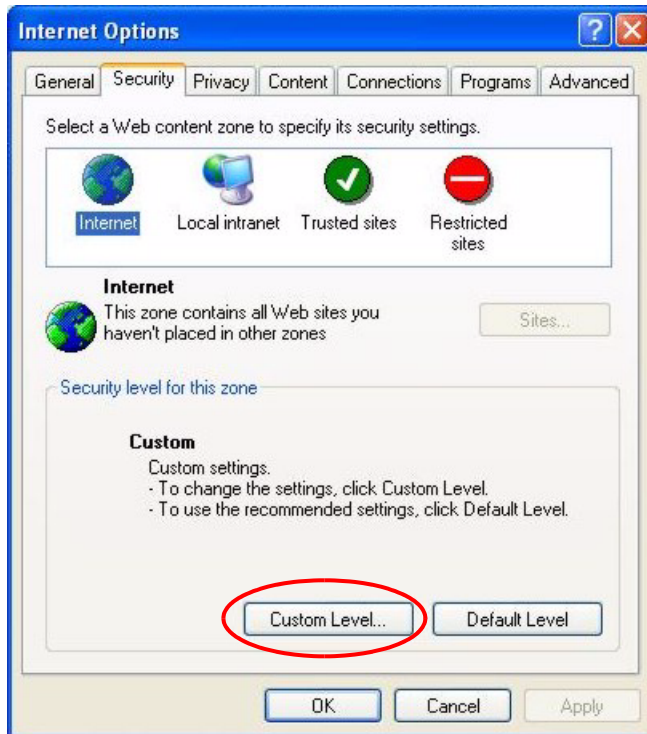
27.4.2 ActiveX Controls in Internet Explorer

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

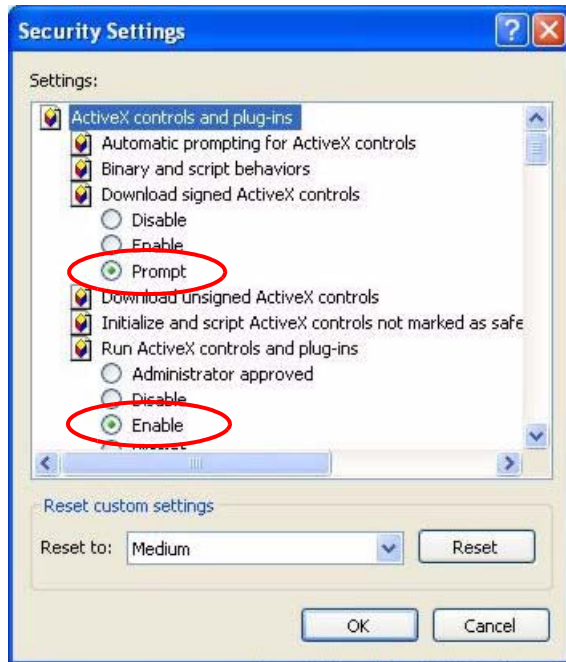
Screen shots for Internet Explorer 6 are shown. Steps may vary depending on your version of Internet Explorer.

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

Figure 212 Internet Options Security



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

Figure 213 Security Setting ActiveX Controls

APPENDIX A

Product Specifications

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

Specification Tables

Table 147 Device

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.32 to 192.168.1.64
Dimensions	(180 W) x (128 D) x (36 H) mm
Weight	P-662HW: 350g; P-662H: 325g
Power Specification	12V AC 1A
Detachable Antenna	Reverse SMA 5dBi
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
Operation Temperature	0° C ~ 40° C
Storage Temperature	-20° ~ 60° C
Operation Humidity	20% ~ 85% RH
Storage Humidity	10% ~ 90% RH

Table 148 Firmware

ADSL Standards	<p>Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G.lite(G.992.2)).</p> <p>ADSL2 G.dmt.bis (G.992.3)</p> <p>ADSL2 G.lite.bis (G.992.4)</p> <p>ADSL2+ (G.992.5)</p> <p>Reach-Extended ADSL (RE ADSL)</p> <p>SRA (Seamless Rate Adaptation)</p> <p>Auto-negotiating rate adaptation</p> <p>ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5)</p> <p>Multi-protocol over AAL5 (RFC2684/1483)</p> <p>PPP over ATM AAL5 (RFC 2364)</p> <p>PPP over Ethernet (RFC 2516)</p> <p>RFC 1483 encapsulation over ATM</p> <p>VC-based and LLC-based multiplexing</p> <p>Up to 8 PVCs (Permanent Virtual Circuits)</p> <p>Remote node for Dial backup</p> <p>I.610 F4/F5 OAM</p> <p>TR.37 compliant auto-configuration using ILM</p>
Other Protocol Support	<p>PPP (Point-to-Point Protocol) link layer protocol.</p> <p>Transparent bridging for unsupported network layer protocols.</p> <p>DHCP Server/Client/Relay</p> <p>RIP I/RIP II</p> <p>ICMP</p> <p>ATM QoS</p> <p>SNMP v1 and v2c with MIB II support (RFC 1213)</p> <p>IP Multicasting IGMP v1 and v2</p> <p>IGMP Proxy</p> <p>UPnP</p>
Management	<p>Embedded Multilingual Web Configurator</p> <p>CLI (Command Line Interpreter)</p> <p>Remote Management via Telnet or Web (TR-069 compliant)</p> <p>CNM v2.2 support</p> <p>SNMP manageable</p> <p>Embedded FTP/TFTP server for firmware downloading, configuration backup and restoration with large rom file support (112K).</p> <p>Syslog</p> <p>Built-in Diagnostic Tools for FLASH memory, ADSL circuitry, RAM and LAN port</p> <p>DeMilitarized Zone (DMZ) Ethernet port provides a way for public servers to be visible to the outside world while still being protected from DoS attacks</p>

Table 148 Firmware (continued)

Wireless (P-662HW only)	<p>IEEE 802.11g Compliance</p> <p>Wireless g+ technology</p> <p>Frequency Range: 2.4 GHz</p> <p>Advanced Orthogonal Frequency Division Multiplexing (OFDM)</p> <p>Data Rates: 108Mbps and Auto Fallback</p> <p>Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit.</p> <p>WLAN bridge to LAN</p> <p>Up to 32 MAC Address filters</p> <p>WPA(2), WPA-PSK</p> <p>Wi-Fi Multimedia specifications (WMM)</p> <p>OTIST (One Touch Intelligent Security Technology)</p> <p>IEEE 802.1x</p> <p>Store up to 32 built-in user profiles using EAP-MD5 (Local User Database)</p> <p>Multiple ESSID</p> <p>External RADIUS server using EAP-MD5, TLS, TTLS</p>
Firewall	<p>Stateful Packet Inspection.</p> <p>Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc.</p> <p>Real time E-mail alerts.</p> <p>Reports and logs.</p>
NAT/SUA	<p>Port Forwarding</p> <p>1024 NAT sessions</p> <p>Multimedia application.</p> <p>PPTP under NAT/SUA.</p> <p>IPSec passthrough</p> <p>SIP ALG passthrough.</p> <p>VPN passthrough</p>
VPN	20 IPSec tunnels.
Content Filtering	Web page blocking by URL keyword.
CAC	Content Access Controls allows user Internet access controls
Static Routes	16 IP and 4 Bridge
Other Features	<p>Any IP</p> <p>SPTGEN</p> <p>Zero Configuration (VC auto-hunting)</p> <p>Traffic Redirect</p> <p>Dynamic DNS</p> <p>IP Alias</p> <p>IP Policy Routing</p> <p>MBM (Multimedia Bandwidth Management) QoS (Quality of Service)</p>

APPENDIX B

About ADSL

Introduction to DSL

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

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

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

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

ADSL Overview

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

Advantages of ADSL

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

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

APPENDIX C

Wall-mounting Instructions

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

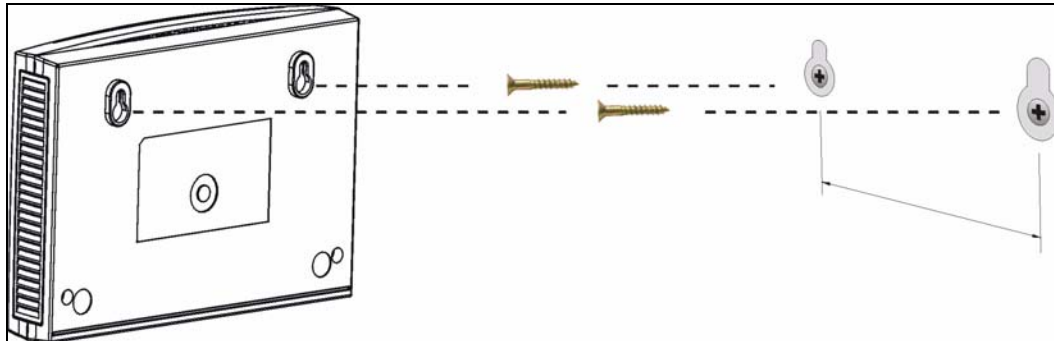
Note: See the product specifications appendix for the size of screws to use and how far apart to place them.

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

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

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

Figure 214 Wall-mounting Example



APPENDIX D

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.

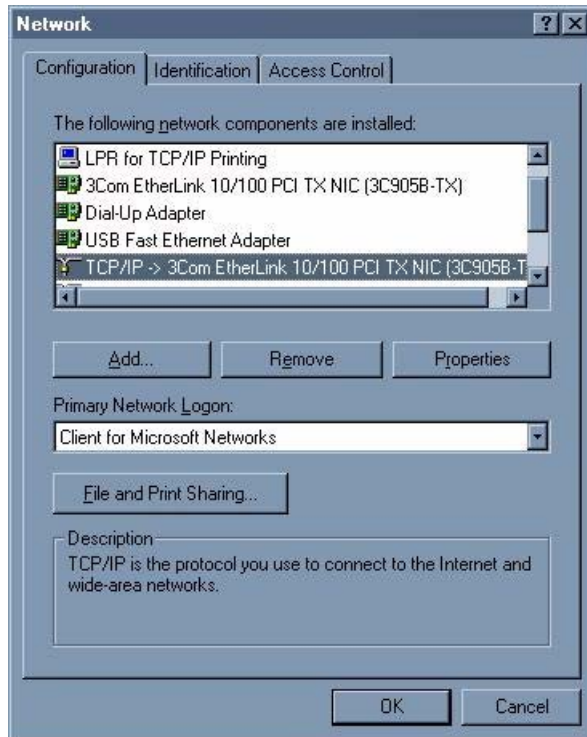
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 215 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:

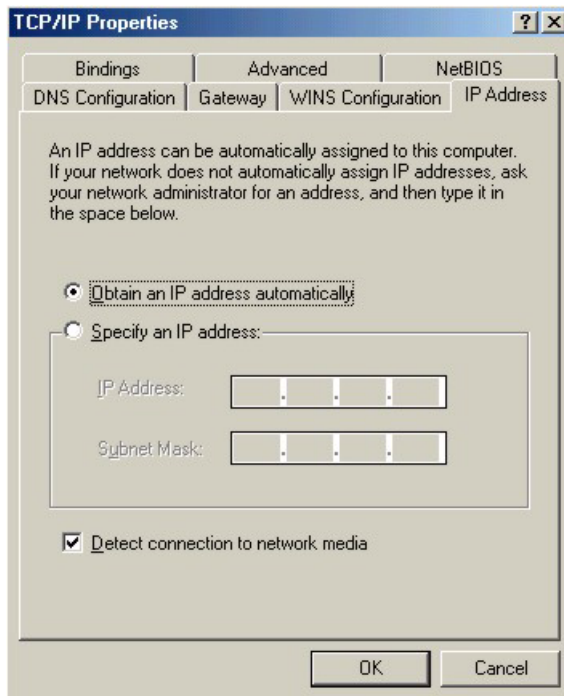
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

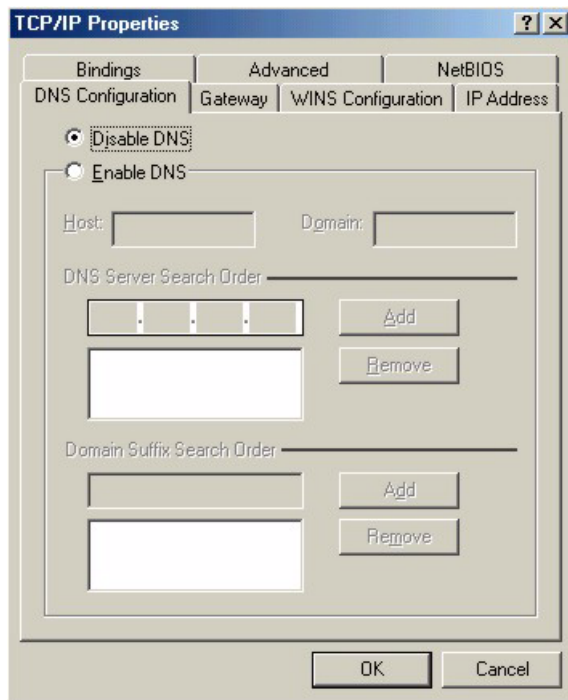
Configuring

- 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 216 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 217 Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Turn on your ZyXEL Device and restart your computer when prompted.

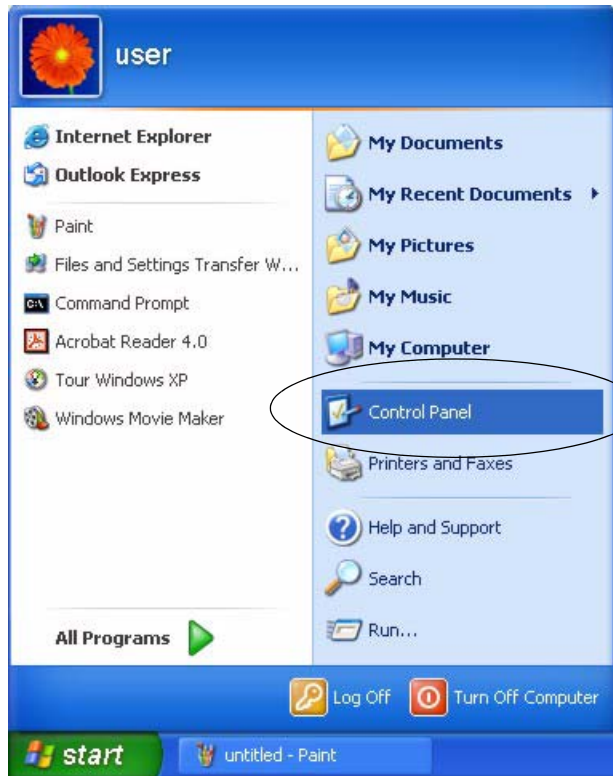
Verifying Settings

1 Click **Start** and then **Run**.**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.**3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

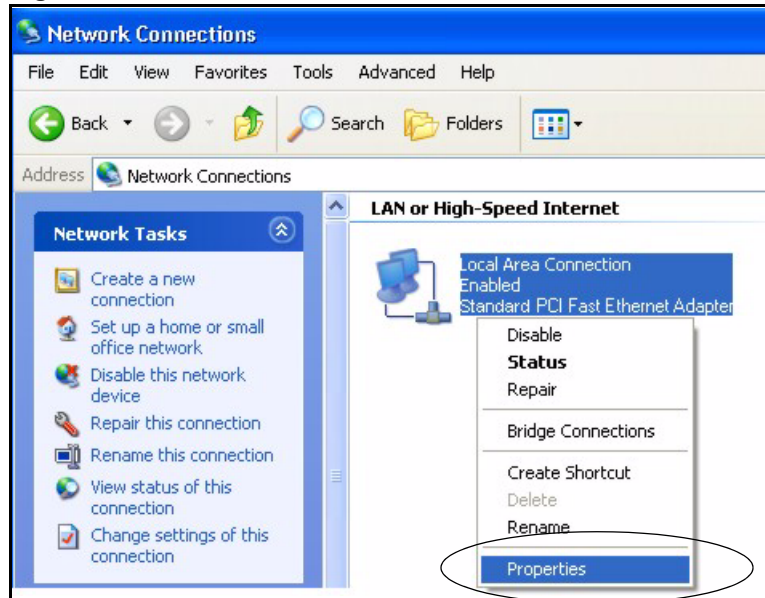
1 Click **start** (**Start** in Windows 2000/NT), **Settings, Control Panel**.

Figure 218 Windows XP: Start Menu

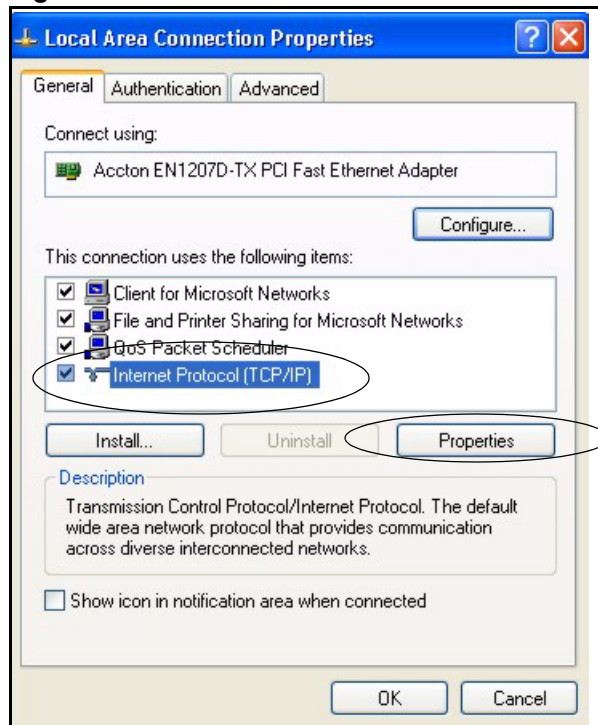
2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

Figure 219 Windows XP: Control Panel

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

Figure 220 Windows XP: Control Panel: Network Connections: Properties

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

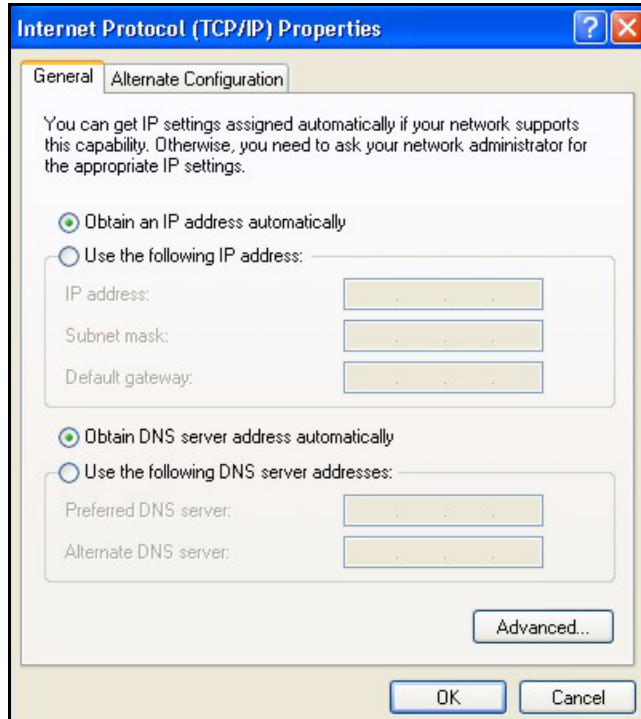
Figure 221 Windows XP: Local Area Connection Properties

- 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**.

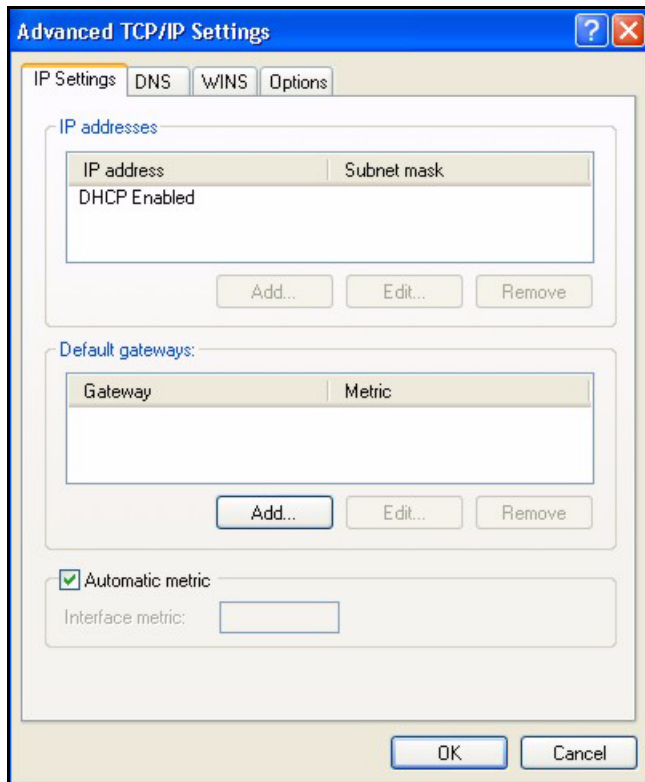
Figure 222 Windows XP: Internet Protocol (TCP/IP) Properties



- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

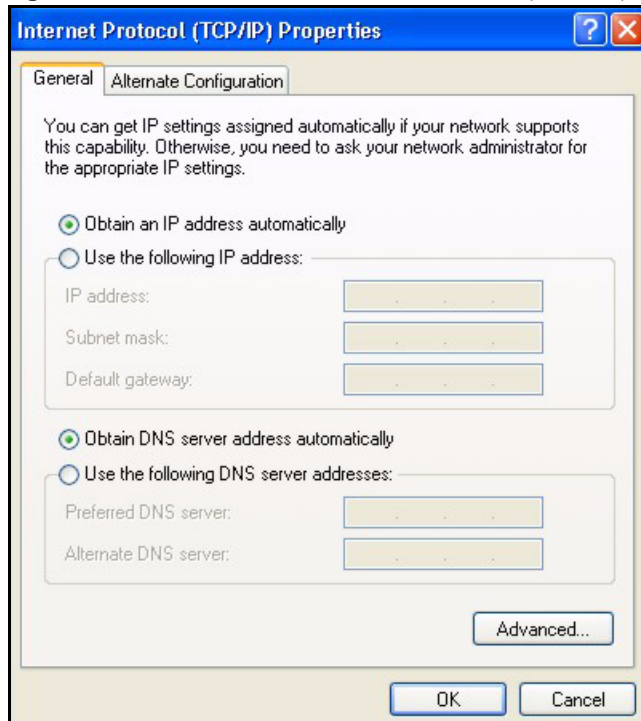
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 223 Windows XP: Advanced TCP/IP Properties

7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 224 Windows XP: Internet Protocol (TCP/IP) Properties

- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.
- 10** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11** Turn on your ZyXEL Device and restart your computer (if prompted).

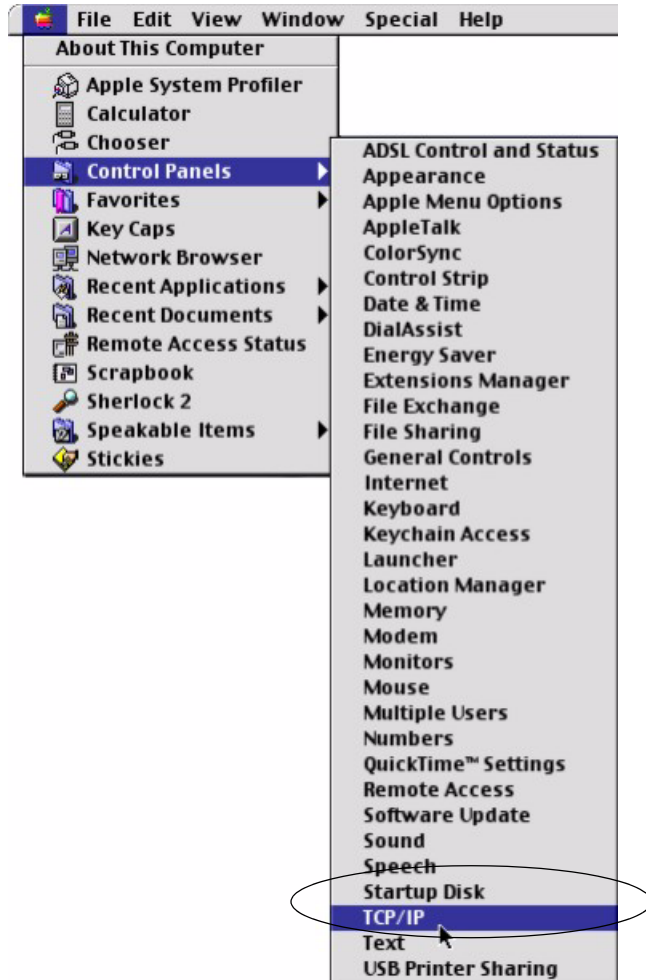
Verifying Settings

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

Macintosh OS 8/9

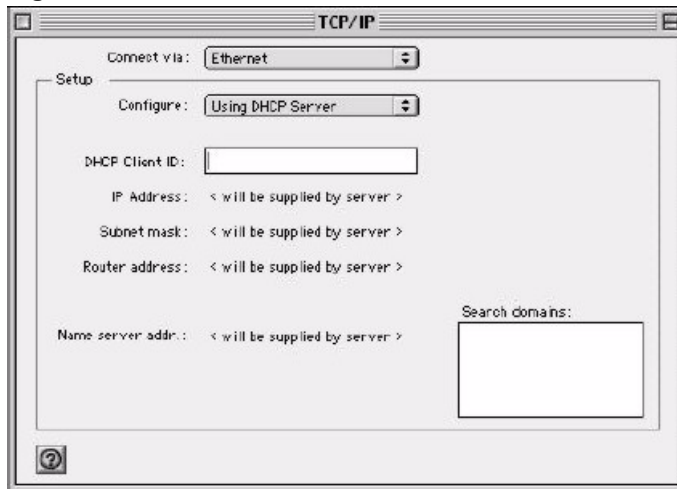
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 225 Macintosh OS 8/9: Apple Menu



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

Figure 226 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).

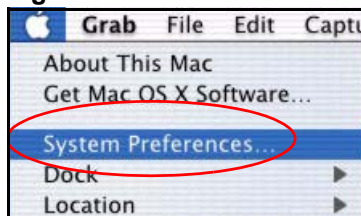
Verifying Settings

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

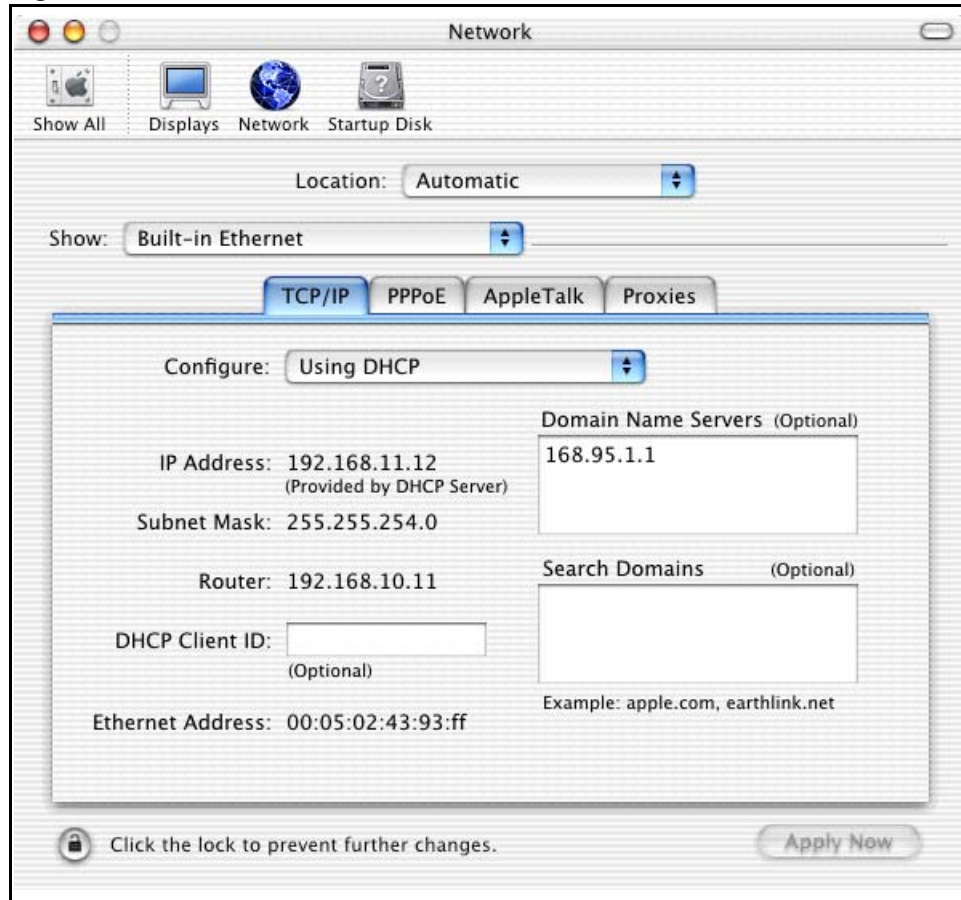
Macintosh OS X

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

Figure 227 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 228 Macintosh OS X: Network

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

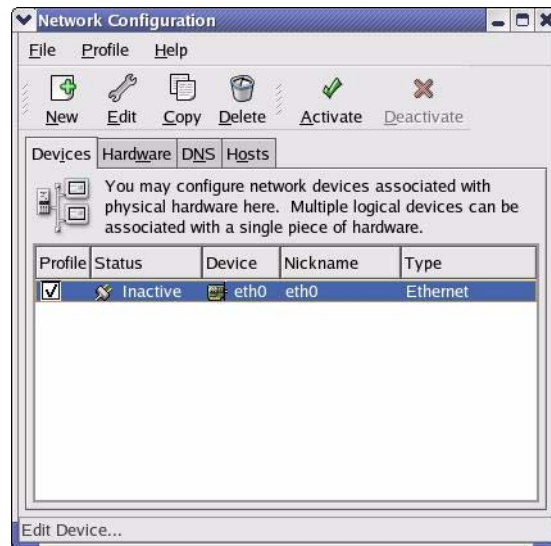
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

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

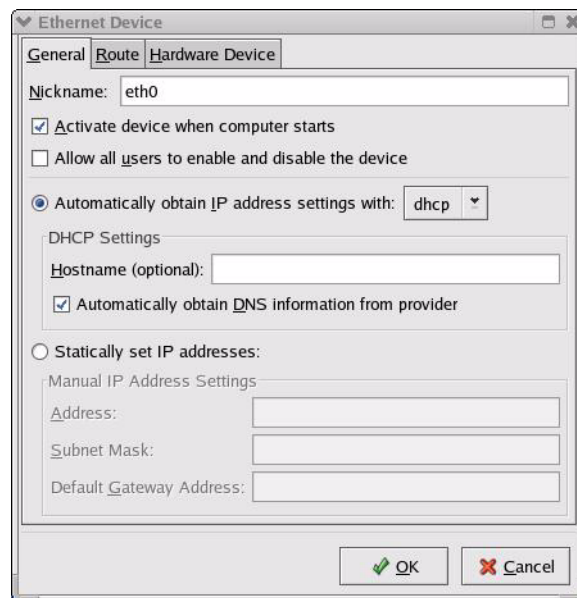
- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 229 Red Hat 9.0: KDE: Network Configuration: Devices



- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 230 Red Hat 9.0: KDE: Ethernet Device: General

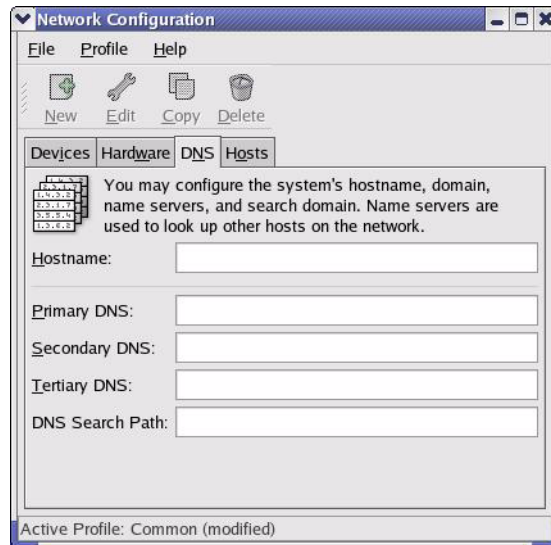


- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

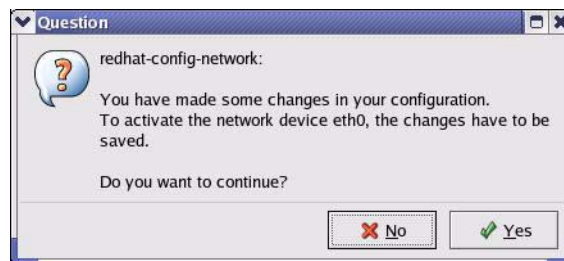
Figure 231 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

Figure 232 Red Hat 9.0: KDE: Network Configuration: Activate



7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
 - If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 233 Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 234 Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 235 Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 236 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 237 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

APPENDIX E

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 149 Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	Network number	Host ID	Host ID	Host ID
Class B	Network number	Network number	Host ID	Host ID
Class C	Network number	Network number	Network number	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have $2^8 - 2$, or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have $2^{16} - 2$, or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have $2^{24} - 2$ hosts, or approximately 16 million hosts.

IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an address.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

Table 150 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 151 “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 152 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 152 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 153 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 154 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	0 0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	1 0000000

Table 154 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 155 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 156 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 156 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 157 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 158 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 159 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 160 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 161 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 149 on page 390](#)) available for subnetting.

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

Table 162 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 F

Wireless LANs

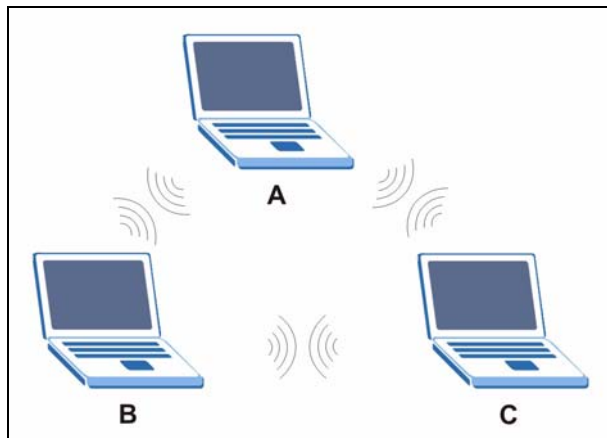
Wireless LAN Topologies

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

Ad-hoc Wireless LAN Configuration

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

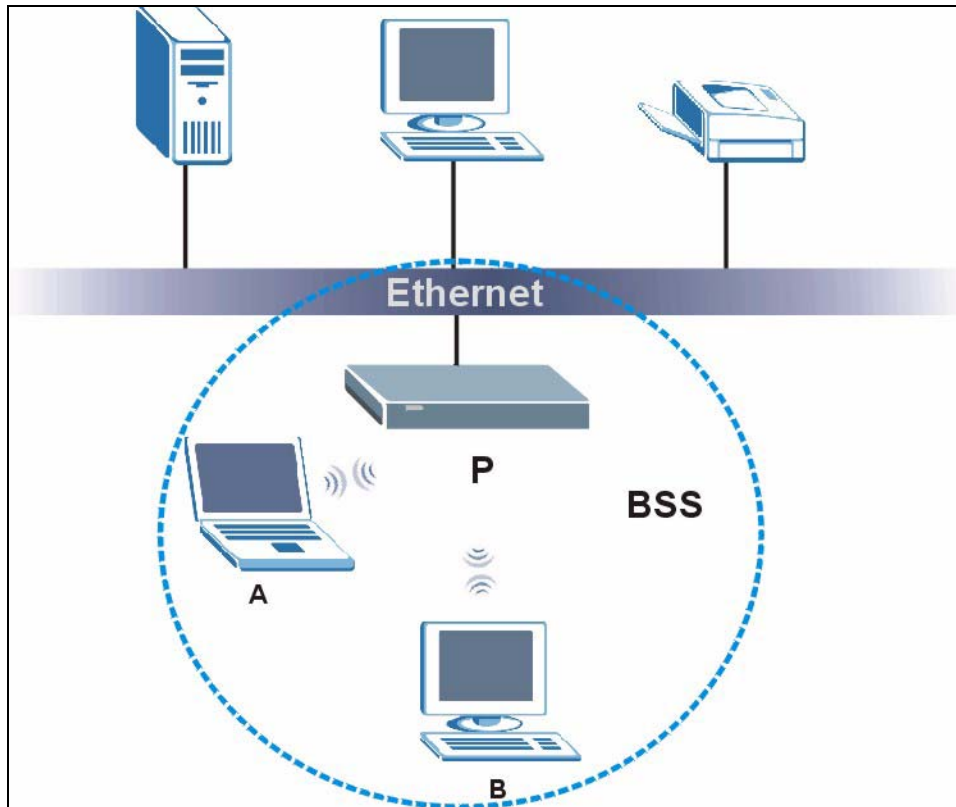
Figure 238 Peer-to-Peer Communication in an Ad-hoc Network



BSS

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

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

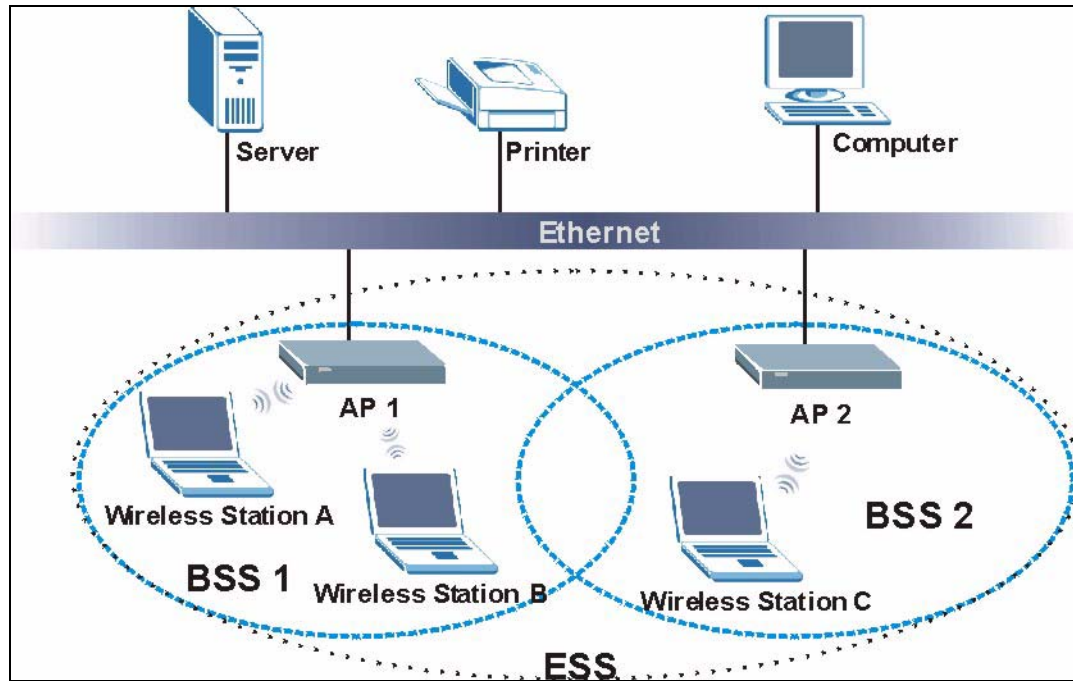
Figure 239 Basic Service Set

ESS

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

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

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

Figure 240 Infrastructure WLAN

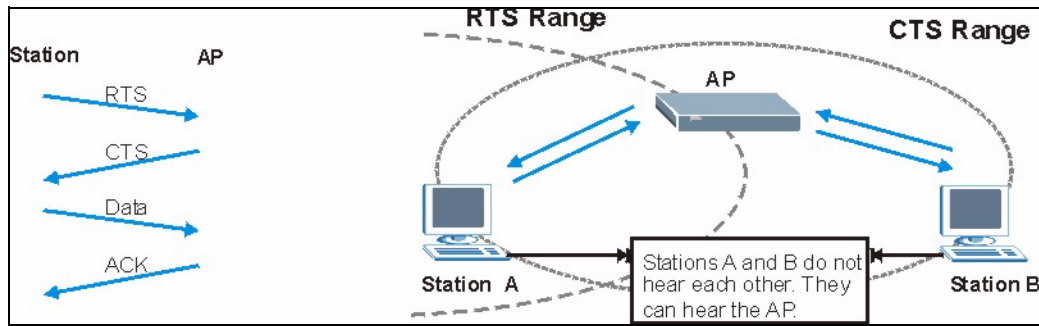
Channel

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

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

RTS/CTS

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

Figure 241 RTS/CTS

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

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

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

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

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

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

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

Fragmentation Threshold

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

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

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

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

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

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

IEEE 802.11g Wireless LAN

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

Table 163 IEEE 802.11g

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

IEEE 802.1x

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

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

RADIUS

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

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

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

Types of RADIUS Messages

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

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.

- Access-Challenge

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

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

- Accounting-Request

Sent by the access point requesting accounting.

- Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

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

Types of Authentication

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

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

EAP-MD5 (Message-Digest Algorithm 5)

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

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

EAP-TLS (Transport Layer Security)

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

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

LEAP

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

Dynamic WEP Key Exchange

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

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

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

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

Table 164 Comparison of EAP Authentication Types

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

WPA(2)

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

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

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

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

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

Encryption

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

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

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

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

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

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

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

User Authentication

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

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

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

Security Parameters Summary

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

Table 165 Wireless Security Relational Matrix

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

APPENDIX G

Importing Certificates

This appendix shows importing certificates examples using Internet Explorer 5.

Import ZyXEL Device Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the ZyXEL Device'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 242 Security Certificate



Importing the ZyXEL Device's Certificate into Internet Explorer

For Internet Explorer to trust a self-signed certificate from the ZyXEL Device, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a ZyXEL Device 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 ZyXEL Device'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 243 Login Screen



2 Click **Install Certificate** to open the **Install Certificate** wizard.

Figure 244 Certificate General Information before Import



3 Click **Next** to begin the **Install Certificate** wizard.

Figure 245 Certificate Import Wizard 1

4 Select where you would like to store the certificate and then click **Next**.

Figure 246 Certificate Import Wizard 2

5 Click **Finish** to complete the **Import Certificate** wizard.

Figure 247 Certificate Import Wizard 3



6 Click **Yes** to add the ZyXEL Device certificate to the root store.

Figure 248 Root Certificate Store

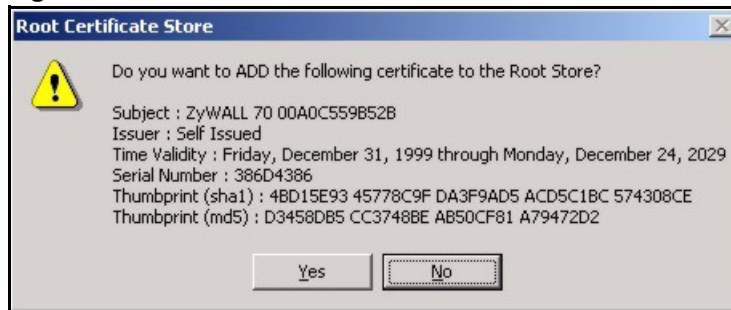


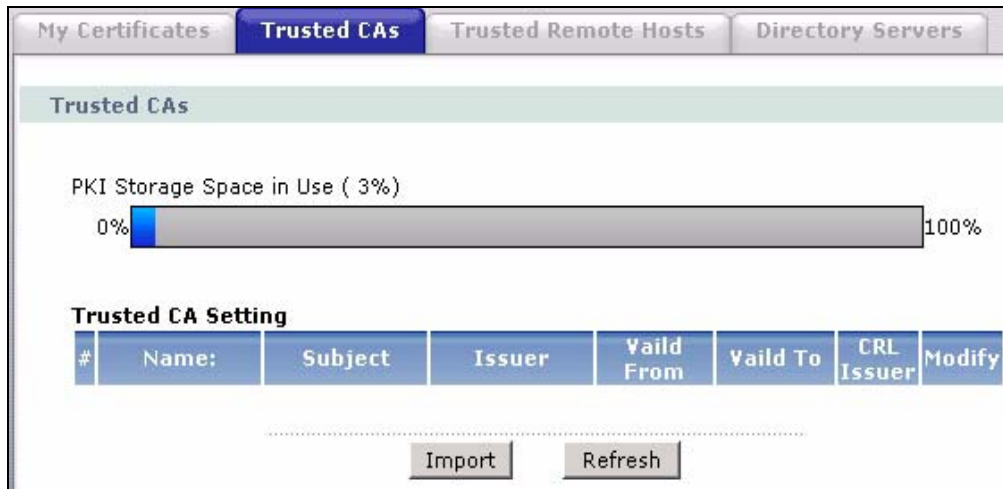
Figure 249 Certificate General Information after Import

Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyXEL Device.

You must have imported at least one trusted CA to the ZyXEL Device in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

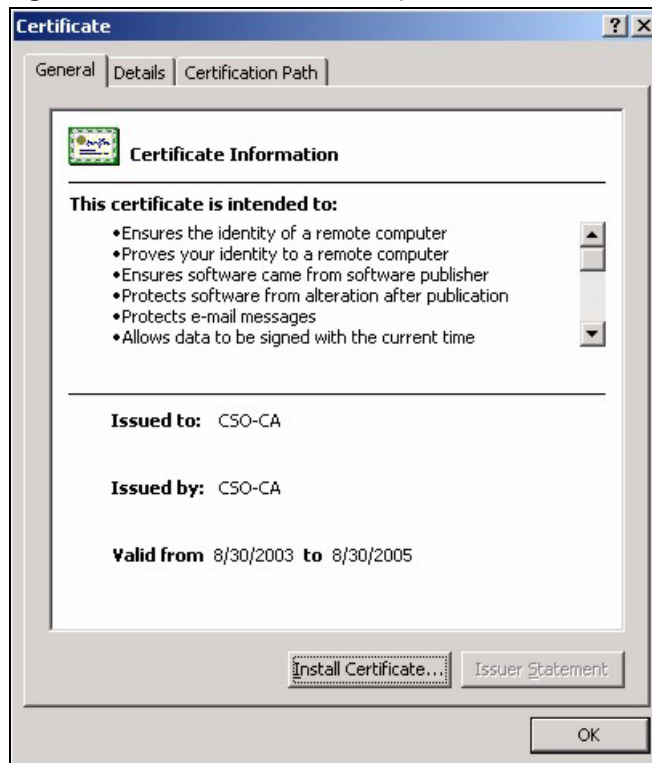
Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyXEL Device (see the ZyXEL Device's **Trusted CA** web configurator screen).

Figure 250 ZyXEL Device 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 251 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 252 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 253 Personal Certificate Import Wizard 2



- 3 Enter the password given to you by the CA.

Figure 254 Personal Certificate Import Wizard 3



- 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 255 Personal Certificate Import Wizard 4



- 5 Click **Finish** to complete the wizard and begin the import process.

Figure 256 Personal Certificate Import Wizard 5

- 6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 257 Personal Certificate Import Wizard 6

Using a Certificate When Accessing the ZyXEL Device Example

Use the following procedure to access the ZyXEL Device via HTTPS.

- 1 Enter 'https://ZyXEL Device IP Address/' in your browser's web address field.

Figure 258 Access the ZyXEL Device Via HTTPS

- 2 When **Authenticate Client Certificates** is selected on the ZyXEL Device, the following screen asks you to select a personal certificate to send to the ZyXEL Device. This screen displays even if you only have a single certificate as in the example.

Figure 259 SSL Client Authentication



3 You next see the ZyXEL Device login screen.

Figure 260 ZyXEL Device Secure Login Screen



APPENDIX H

Command Interpreter

The following describes how to use the command interpreter.

Note: Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

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

For example,

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

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

Access via Telnet

Use the following steps to telnet into your ZyXEL Device.

- 1** Make sure that your computer is physically connected to one of the LAN ports.
- 2** Make sure your computer IP address and the switch IP address are on the same subnet. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type `telnet 192.168.1.1` (the default management IP address) and click **OK**.
- 3** A login screen displays. Enter the administrative password to login (default password is **1234**).

Command Usage

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

APPENDIX I

Certificates Commands

The following describes the certificate commands. See [Appendix H on page 419](#) for information on the command structure.

All of these commands start with certificates.

Table 166 Certificates Commands

COMMAND	DESCRIPTION		
my_cert			
	create		
	create	selfsigned <name> <subject> [key size]	Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn:{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	create	request <name> <subject> [key size]	Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn:{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	create	scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn:{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.

Table 166 Certificates Commands (continued)

COMMAND	DESCRIPTION		
	create	cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ".". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn:{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	import	[name]	Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	delete	<name>	Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted.
	list		List all my certificate names and basic information.
	rename	<old name> <new name>	Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	def_self_signed	[name]	Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed.

Table 166 Certificates Commands (continued)

COMMAND	DESCRIPTION		
	replace_factory		Create a certificate using your device MAC address that will be specific to this device. The factory default certificate is a common default certificate for all ZyWALL models.
ca_trusted			
	import	<name>	Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	delete	<name>	Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
	list		List all trusted CA certificate names and basic information.
	rename	<old name> <new name>	Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	crl_issuer	<name> [on off]	Specify whether or not the specified CA issues CRL. <name> specifies the name of the CA certificate. [on off] specifies whether or not the CA issues CRL. If [on off] is not specified, the current crl_issuer status of the CA.
remote_trusted			
	import	<name>	Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host certificate is to be saved.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.

Table 166 Certificates Commands (continued)

COMMAND	DESCRIPTION		
	delete	<name>	Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted.
	list		List all trusted remote host certificate names and basic information.
	rename	<old name> <new name>	Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
dir_server			
	add	<name> <addr[:port]> > [login:pswd]	Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
	delete	<name>	Delete the specified directory service. <name> specifies the name of the directory server to be deleted.
	view	<name>	View the specified directory service. <name> specifies the name of the directory server to be viewed.
	edit	<name> <addr[:port]> > [login:pswd]	Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
	list		List all directory service names and basic information.
	rename	<old name> <new name>	Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.
cert_manager			
	reinit		Reinitialize the certificate manager.

APPENDIX J

Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware is started. When you start up your ZyXEL Device, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the **Firmware and Configuration File Maintenance** chapter.

Figure 261 Option to Enter Debug Mode

```
Bootbase Version: V1.02 | 08/08/2001 15:40:50
RAM: Size = 16384 Kbytes
DRAM Post: Testing: 16384K OK
FLASH: Intel 16M
RAS Version: V3.50(WB.0)b3 | 08/08/2001 16:21:27
Press any key to enter debug mode within 3
seconds.
.....
```

Enter ATHE to view all available ZyXEL Device boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

Figure 262 Boot Module Commands

AT	just answer OK
ATHE	print help
ATBAx	change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx, (y)	set BootExtension Debug Flag (y=password)
ATSE	show the seed of password generator
ATTI(h,m,s)	change system time to hour:min:sec or show current time
ATDA(y,m,d)	change system date to year/month/day or show current date
ATDS	dump RAS stack
ATDT	dump Boot Module Common Area
ATDUx,y	dump memory contents from address x for length y
ATRBx	display the 8-bit value of address x
ATRWx	display the 16-bit value of address x
ATRLx	display the 32-bit value of address x
ATGO(x)	run program at addr x or boot router
ATGR	boot router
ATGT	run Hardware Test Program
ATRTw,x,y(,z)	RAM test level w, from address x to y (z iterations)
ATSH	dump manufacturer related data in ROM
ATDOx,y	download from address x for length y to PC via XMODEM
ATTD	download router configuration to PC via XMODEM
ATUR	upload router firmware to flash ROM
ATLC	upload router configuration file to flash ROM
ATXSx	xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSR	system reboot

APPENDIX K

Firewall Commands

The following describes the firewall commands.

Table 167 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
Firewall SetUp		
	<code>config edit firewall active <yes no></code>	This command turns the firewall on or off.
	<code>config retrieve firewall</code>	This command returns the previously saved firewall settings.
	<code>config save firewall</code>	This command saves the current firewall settings.
Display		
	<code>config display firewall</code>	This command shows the of all the firewall settings including e-mail, attack, and the sets/ rules.
	<code>config display firewall set <set #></code>	This command shows the current configuration of a set; including timeout values, name, default-permit, and etc.If you don't put use a number (#) after "set", information about all of the sets/rules appears.
	<code>config display firewall set <set #> rule <rule #></code>	This command shows the current entries of a rule in a firewall rule set.
	<code>config display firewall attack</code>	This command shows all of the attack response settings.
	<code>config display firewall e-mail</code>	This command shows all of the e-mail settings.
	<code>config display firewall?</code>	This command shows all of the available firewall sub commands.
Edit		

Table 167 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
E-mail	<code>config edit firewall e-mail mail-server <ip address of mail server></code>	This command sets the IP address to which the e-mail messages are sent.
	<code>config edit firewall e-mail return-addr <e-mail address></code>	This command sets the source e-mail address of the firewall e-mails.
	<code>config edit firewall e-mail email-to <e-mail address></code>	This command sets the e-mail address to which the firewall e-mails are sent.
	<code>config edit firewall e-mail policy <full hourly daily weekly></code>	This command sets how frequently the firewall log is sent via e-mail.
	<code>config edit firewall e-mail day <sunday monday tuesday wednesday thursday friday saturday></code>	This command sets the day on which the current firewall log is sent through e-mail if the ZyXEL Device is set to send it on a weekly basis.
	<code>config edit firewall e-mail hour <0-23></code>	This command sets the hour when the firewall log is sent through e-mail if the ZyXEL Device is set to send it on an hourly, daily or weekly basis.
	<code>config edit firewall e-mail minute <0-59></code>	This command sets the minute of the hour for the firewall log to be sent via e-mail if the ZyXEL Device is set to send it on a hourly, daily or weekly basis.
Attack	<code>config edit firewall attack send-alert <yes no></code>	This command enables or disables the immediate sending of DOS attack notification e-mail messages.
	<code>config edit firewall attack block <yes no></code>	Set this command to yes to block new traffic after the tcp-max-incomplete threshold is exceeded. Set it to no to delete the oldest half-open session when traffic exceeds the tcp-max-incomplete threshold.
	<code>config edit firewall attack block-minute <0-255></code>	This command sets the number of minutes for new sessions to be blocked when the tcp-max-incomplete threshold is reached. This command is only valid when block is set to yes.

Table 167 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	<code>config edit firewall attack minute-high <0-255></code>	This command sets the threshold rate of new half-open sessions per minute where the ZyXEL Device starts deleting old half-opened sessions until it gets them down to the minute-low threshold.
	<code>config edit firewall attack minute-low <0-255></code>	This command sets the threshold of half-open sessions where the ZyXEL Device stops deleting half-opened sessions.
	<code>config edit firewall attack max-incomplete-high <0-255></code>	This command sets the threshold of half-open sessions where the ZyXEL Device starts deleting old half-opened sessions until it gets them down to the max incomplete low.
	<code>config edit firewall attack max-incomplete-low <0-255></code>	This command sets the threshold where the ZyXEL Device stops deleting half-opened sessions.
	<code>config edit firewall attack tcp-max-incomplete <0-255></code>	This command sets the threshold of half-open TCP sessions with the same destination where the ZyXEL Device starts dropping half-open sessions to that destination.
Sets	<code>config edit firewall set <set #> name <desired name></code>	This command sets a name to identify a specified set.
	<code>Config edit firewall set <set #> default-permit <forward block></code>	This command sets whether a packet is dropped or allowed through, when it does not meet a rule within the set.
	<code>Config edit firewall set <set #> icmp-timeout <seconds></code>	This command sets the time period to allow an ICMP session to wait for the ICMP response.
	<code>Config edit firewall set <set #> udp-idle-timeout <seconds></code>	This command sets how long a UDP connection is allowed to remain inactive before the ZyXEL Device considers the connection closed.
	<code>Config edit firewall set <set #> connection-timeout <seconds></code>	This command sets how long ZyXEL Device waits for a TCP session to be established before dropping the session.
	<code>Config edit firewall set <set #> fin-wait-timeout <seconds></code>	This command sets how long the ZyXEL Device leaves a TCP session open after the firewall detects a FIN-exchange (indicating the end of the TCP session).

Table 167 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	Config edit firewall set <set #> tcp-idle-timeout <seconds>	This command sets how long ZyXEL Device lets an inactive TCP connection remain open before considering it closed.
	Config edit firewall set <set #> log <yes no>	This command sets whether or not the ZyXEL Device creates logs for packets that match the firewall's default rule set.
Rules	Config edit firewall set <set #> rule <rule #> permit <forward block>	This command sets whether packets that match this rule are dropped or allowed through.
	Config edit firewall set <set #> rule <rule #> active <yes no>	This command sets whether a rule is enabled or not.
	Config edit firewall set <set #> rule <rule #> protocol <integer protocol value >	This command sets the protocol specification number made in this rule for ICMP.
	Config edit firewall set <set #> rule <rule #> log <none match not-match both>	This command sets the ZyXEL Device to log traffic that matches the rule, doesn't match, both or neither.
	Config edit firewall set <set #> rule <rule #> alert <yes no>	This command sets whether or not the ZyXEL Device sends an alert e-mail when a DOS attack or a violation of a particular rule occurs.
	config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>	This command sets the rule to have the ZyXEL Device check for traffic with this individual source address.
	config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>	This command sets a rule to have the ZyXEL Device check for traffic from a particular subnet (defined by IP address and subnet mask).
	config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>	This command sets a rule to have the ZyXEL Device check for traffic from this range of addresses.

Table 167 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	<code>config edit firewall set <set #> rule <rule #> destaddr-single <ip address></code>	This command sets the rule to have the ZyXEL Device check for traffic with this individual destination address.
	<code>config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask></code>	This command sets a rule to have the ZyXEL Device check for traffic with a particular subnet destination (defined by IP address and subnet mask).
	<code>config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address></code>	This command sets a rule to have the ZyXEL Device check for traffic going to this range of addresses.
	<code>config edit firewall set <set #> rule <rule #> TCP destport-single <port #></code>	This command sets a rule to have the ZyXEL Device check for TCP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	<code>config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #></code>	This command sets a rule to have the ZyXEL Device check for TCP traffic with a destination port in this range.
	<code>config edit firewall set <set #> rule <rule #> UDP destport-single <port #></code>	This command sets a rule to have the ZyXEL Device check for UDP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	<code>config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #></code>	This command sets a rule to have the ZyXEL Device check for UDP traffic with a destination port in this range.
Delete		
	<code>config delete firewall e-mail</code>	This command removes all of the settings for e-mail alert.
	<code>config delete firewall attack</code>	This command resets all of the attack response settings to their defaults.
	<code>config delete firewall set <set #></code>	This command removes the specified set from the firewall configuration.

Table 167 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	<code>config delete firewall set <set #> rule<rule #></code>	This command removes the specified rule in a firewall configuration set.

APPENDIX L

NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands.

Introduction

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

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

You can configure NetBIOS filters to do the following:

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

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

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

NetBIOS Display Filter Settings Command Example

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

The filter types and their default settings are as follows.

Table 168 NetBIOS Filter Default Settings

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

NetBIOS Filter Configuration

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

where

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

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

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

Example commands

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

~~`sys filter netbios config 1 off`~~ This command forwards LAN to DMZ and DMZ to LAN NetBIOS packets.

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

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

APPENDIX M

Internal SPTGEN

Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple ZyXEL Device. 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 SMT menus 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 263 Configuration Text File Format: Column Descriptions

```
/ Menu 1 General Setup
10000000 = Configured           <0 (No) | 1 (Yes)>      = 1
10000001 = System Name         <Str>                  = ZyXEL
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.

For more text file examples, refer to the *Example Internal SPTGEN Screens Appendix*.

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 263 on page 437](#)), 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 264 on page 438](#), 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 263 on page 437](#)).

Figure 264 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 265 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 266 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 267 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 169 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number (not seen in SMT screens)
FN	Field Name

Table 169 Abbreviations Used in the Example Internal SPTGEN Screens Table (continued)

ABBREVIATION	MEANING
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the ZyXEL Device.

The following are Internal SPTGEN screens associated with the SMT screens of your ZyXEL Device.

Table 170 Menu 1 General Setup (SMT Menu 1)

/ Menu 1 General Setup (SMT Menu 1)			
FIN	FN	PVA	INPUT
10000000 =	Configured	<0 (No) 1 (Yes)>	= 0
10000001 =	System Name	<Str>	= ZyXEL
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 171 Menu 3 (SMT Menu 3)

/ Menu 3.1 General Ethernet Setup (SMT menu 3.1)			
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

Table 171 Menu 3 (SMT Menu 3 (continued))

/ Menu 3.2 TCP/IP and DHCP Ethernet Setup (SMT Menu 3.2)			
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 (SMT Menu 3.2.1)			
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 171 Menu 3 (SMT Menu 3 (continued))

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 (SMT Menu 3.5)				
	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 171 Menu 3 (SMT Menu 3 (continued))

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 (SMT MENU 3.5.1)			
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 172 Menu 4 Internet Access Setup (SMT Menu 4)

/ Menu 4 Internet Access Setup (SMT Menu 4)			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0 (No) 1 (Yes)>	= 1
40000001 =	ISP	<0 (No) 1 (Yes)>	= 1

Table 172 Menu 4 Internet Access Setup (SMT Menu 4) (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 172 Menu 4 Internet Access Setup (SMT Menu 4) (continued)

40000032=	RIP Version	<0 (Rip-1) 1 (Rip-2B) 2 (Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0 (No) 1 (Yes)>	= 0

Table 173 Menu 12 (SMT Menu 12)

/ Menu 12.1.1 IP Static Route Setup (SMT Menu 12.1.1)			
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 (SMT Menu 12.1.2)			
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 (SMT Menu 12.1.3)			
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 173 Menu 12 (SMT Menu 12) (continued)

/ Menu 12.1.4 IP Static Route Setup (SMT Menu 12.1.4)			
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 (SMT Menu 12.1.5)			
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 (SMT Menu 12.1.6)			
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 (SMT Menu 12.1.7)			
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 173 Menu 12 (SMT 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 (SMT Menu 12.1.8)			
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 (SMT Menu 12.1.9)			
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 (SMT Menu 12.1.10)			
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 (SMT Menu 12.1.11)			
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 173 Menu 12 (SMT 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 (SMT Menu 12.1.12)			
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 (SMT Menu 12.1.13)			
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 (SMT Menu 12.1. 14)			
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 (SMT Menu 12.1. 15)			
FIN	FN	PVA	INPUT
120115001 =	IP Static Route set #15, Name	<Str>	=

Table 173 Menu 12 (SMT 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 (SMT Menu 12.1. 16)			
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 174 Menu 15 SUA Server Setup (SMT Menu 15)

/ Menu 15 SUA Server Setup (SMT Menu 15)			
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 174 Menu 15 SUA Server Setup (SMT Menu 15) (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 174 Menu 15 SUA Server Setup (SMT Menu 15) (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 175 Menu 21.1 Filter Set #1 (SMT Menu 21.1)

/ Menu 21 Filter set #1 (SMT Menu 21)			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=
/ Menu 21.1.1.1 set #1, rule #1 (SMT Menu 21.1.1.1)			
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 175 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

/ Menu 21.1.1.2 set #1, rule #2 (SMT Menu 21.1.1.2)			
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 (SMT Menu 21.1.1.3)			
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 175 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (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 (SMT Menu 21.1.1.4)			
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 (SMT Menu 21.1.1.5)			
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 175 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (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 (SMT Menu 21.1.1.6)			
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 176 Menu 21.1 Filer Set #2, (SMT Menu 21.1)

/ Menu 21.1 filter set #2, (SMT Menu 21.1)			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN

Table 176 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

/ Menu 21.1.2.1 Filter set #2, rule #1 (SMT Menu 21.1.2.1)			
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 (SMT Menu 21.1.2.2)			
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 176 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (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 (SMT Menu 21.1.2.3)			
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 (SMT Menu 21.1.2.4)			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type	<0 (none) 2 (TCP/IP)>	= 2

Table 176 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (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 (SMT Menu 21.1.2.5)			
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 176 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (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 (SMT Menu 21.1.2.5)			
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 177 Menu 23 System Menus (SMT Menu 23)

*/ Menu 23.1 System Password Setup (SMT Menu 23.1)			
FIN	FN	PVA	INPUT
230000000 =	System Password		= 1234
*/ Menu 23.2 System security: radius server (SMT Menu 23.2)			
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: IEEE 802.1x (SMT Menu 23.4)			
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 177 Menu 23 System Menus (SMT Menu 23) (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 178 Menu 24.11 Remote Management Control (SMT Menu 24.11)

/ Menu 24.11 Remote Management Control (SMT Menu 24.11)			
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 179 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 179 Command Examples (continued)

	FIN	FN	PVA	INPUT
	FIN	FN	PVA	INPUT
	990000001 =	ADSL OPMD	<0(etsi) 1(normal) 2(gdmt) 3(multimo de)>	= 3

APPENDIX N

Splitters and Microfilters

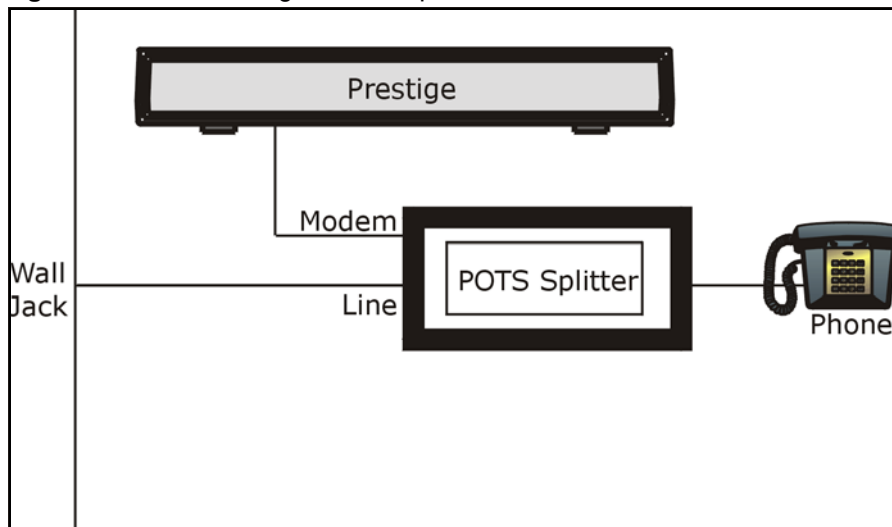
This appendix tells you how to install a POTS splitter or a telephone microfilter.

Connecting a POTS Splitter

When you use the Full Rate (G.dmt) ADSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitter at the point where the telephone line enters your residence, as shown in the following figure.

Figure 268 Connecting a POTS Splitter



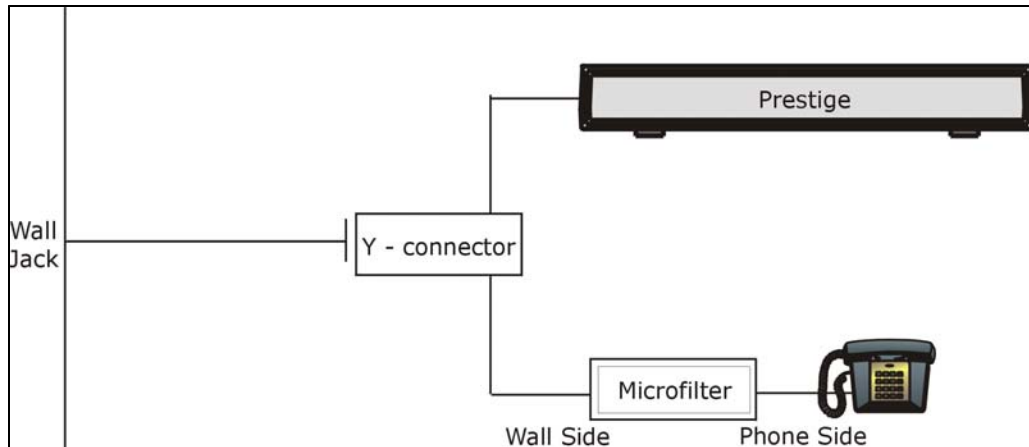
- 1 Connect the side labeled “Phone” to your telephone.
- 2 Connect the side labeled “Modem” “DSL” to your ZyXEL Device.
- 3 Connect the side labeled “Line” to the telephone wall jack.

Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.

- 1 Connect a phone cable from the wall jack to the single jack end of the Y- Connector.
- 2 Connect a cable from the double jack end of the Y-Connector to the “wall side” of the microfilter.
- 3 Connect another cable from the double jack end of the Y-Connector to the ZyXEL Device.
- 4 Connect the “phone side” of the microfilter to your telephone as shown in the following figure.

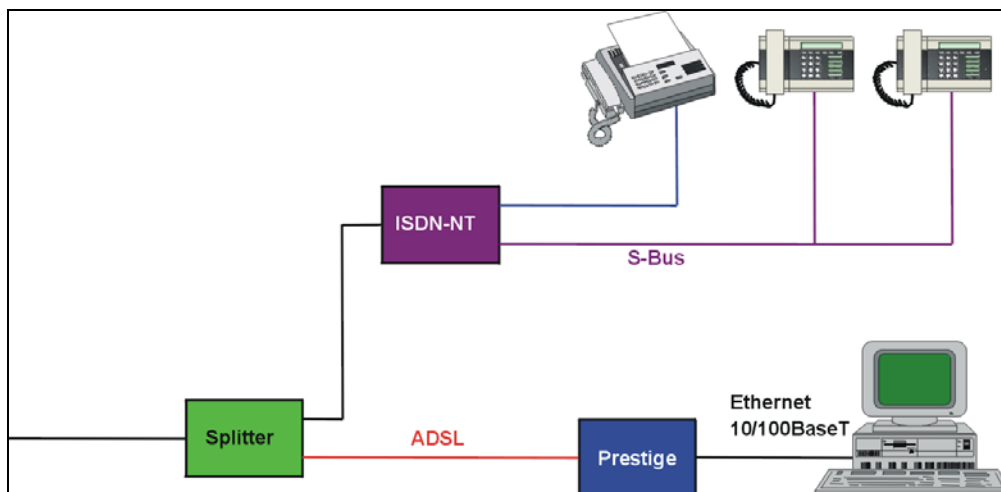
Figure 269 Connecting a Microfilter



ZyXEL Device With ISDN

This section relates to people who use their ZyXEL Device with ADSL over ISDN (digital telephone service) only. The following is an example installation for the ZyXEL Device with ISDN.

Figure 270 ZyXEL Device with ISDN



APPENDIX O

Log Descriptions

This appendix provides descriptions of example log messages.

Table 180 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 180 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 181 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 182 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 183 TCP Reset Logs

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

Table 184 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[TCP UDP ICMP IGMP Generic] packet filter matched (set:%d, rule:%d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

Table 185 ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting. For type and code details, see Table 197 on page 477 .
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 197 on page 477 .
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 186 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 187 PPP Logs

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

Table 187 PPP Logs (continued)

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

Table 188 UPnP Logs

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

Table 189 Content Filtering Logs

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

Table 189 Content Filtering Logs (continued)

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

Table 190 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack. For type and code details, see Table 197 on page 477 .
land [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack. For type and code details, see Table 197 on page 477 .
ip spoofing - WAN [TCP UDP IGMP ESP GRE OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 197 on page 477 .
icmp echo: ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 197 on page 477 .
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack. For type and code details, see Table 197 on page 477 .
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP UDP IGMP ESP GRE OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 197 on page 477 .
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack. For type and code details, see Table 197 on page 477 .

Table 191 IPsec Logs

LOG MESSAGE	DESCRIPTION
Discard REPLAY packet	The router received and discarded a packet with an incorrect sequence number.
Inbound packet authentication failed	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
Receive IPsec packet, but no corresponding tunnel exists	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
Rule <%d> idle time out, disconnect	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CLI command to set the time period. The default value is 2 minutes.
WAN IP changed to <IP>	The router dropped all connections with the "MyIP" configured as "0.0.0.0" when the WAN IP address changed.

Table 192 IKE Logs

LOG MESSAGE	DESCRIPTION
Active connection allowed exceeded	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
Start Phase 2: Quick Mode	Phase 2 Quick Mode has started.
Verifying Remote ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
Verifying Local ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
IKE Packet Retransmit	The router retransmitted the last packet sent because there was no response from the peer.
Failed to send IKE Packet	An Ethernet error stopped the router from sending IKE packets.
Too many errors! Deleting SA	An SA was deleted because there were too many errors.
Phase 1 IKE SA process done	The phase 1 IKE SA process has been completed.
Duplicate requests with the same cookie	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
IKE Negotiation is in process	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
No proposal chosen	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
Local / remote IPs of incoming request conflict with rule <%d>	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.

Table 192 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Cannot resolve Secure Gateway Addr for rule <%d>	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
Peer ID: <peer id> <My remote type> -<My local type>	The displayed ID information did not match between the two ends of the connection.
vs. My Remote <My remote> - <My remote>	The displayed ID information did not match between the two ends of the connection.
vs. My Local <My local>-<My local>	The displayed ID information did not match between the two ends of the connection.
Send <packet>	A packet was sent.
Recv <packet>	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
Recv <Main or Aggressive> Mode request from <IP>	The router received an IKE negotiation request from the peer address specified.
Send <Main or Aggressive> Mode request to <IP>	The router started negotiation with the peer.
Invalid IP <Peer local> / <Peer local>	The peer's "Local IP Address" is invalid.
Remote IP <Remote IP> / <Remote IP> conflicts	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Phase 1 ID type mismatch	This router's "Peer ID Type" is different from the peer IPsec router's "Local ID Type".
Phase 1 ID content mismatch	This router's "Peer ID Content" is different from the peer IPsec router's "Local ID Content".
No known phase 1 ID type found	The router could not find a known phase 1 ID in the connection attempt.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	The phase 1 ID types do not match.
ID content mismatch	The phase 1 ID contents do not match.
Configured Peer ID Content: <Configured Peer ID Content>	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
Incoming ID Content: <Incoming Peer ID Content>	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
Unsupported local ID Type: <%d>	The phase 1 ID type is not supported by the router.
Build Phase 1 ID	The router has started to build the phase 1 ID.
Adjust TCP MSS to%d	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
Rule <%d> input idle time out, disconnect	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
XAUTH succeed! Username: <Username>	The router used extended authentication to authenticate the listed username.

Table 192 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed username.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication algorithm mismatch	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication method mismatch	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
Rule [%d] Phase 1 key group mismatch	The listed rule's IKE phase 1 key group did not match between the router and the peer.
Rule [%d] Phase 2 protocol mismatch	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
Rule [%d] Phase 2 encryption algorithm mismatch	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 2 authentication algorithm mismatch	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 2 encapsulation mismatch	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
Rule [%d]> Phase 2 pfs mismatch	The listed rule's IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.
Rule [%d] Phase 1 ID mismatch	The listed rule's IKE phase 1 ID did not match between the router and the peer.
Rule [%d] Phase 1 hash mismatch	The listed rule's IKE phase 1 hash did not match between the router and the peer.
Rule [%d] Phase 1 preshared key mismatch	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
Rule [%d] Tunnel built successfully	The listed rule's IPsec tunnel has been built successfully.
Rule [%d] Peer's public key not found	The listed rule's IKE phase 1 peer's public key was not found.
Rule [%d] Verify peer's signature failed	The listed rule's IKE phase 1 verification of the peer's signature failed.
Rule [%d] Sending IKE request	IKE sent an IKE request for the listed rule.
Rule [%d] Receiving IKE request	IKE received an IKE request for the listed rule.
Swap rule to rule [%d]	The router changed to using the listed rule.
Rule [%d] Phase 1 key length mismatch	The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
Rule [%d] phase 1 mismatch	The listed rule's IKE phase 1 did not match between the router and the peer.

Table 192 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] phase 2 mismatch	The listed rule's IKE phase 2 did not match between the router and the peer.
Rule [%d] Phase 2 key length mismatch	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.

Table 193 PKI Logs

LOG MESSAGE	DESCRIPTION
Enrollment successful	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
Enrollment failed	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <SCEP CA server url>	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
Enrollment successful	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
Enrollment failed	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <CMP CA server url>	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
Rcvd ca cert: <subject name>	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd user cert: <subject name>	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd CRL <size>: <issuer name>	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd ARL <size>: <issuer name>	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ca cert	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received user cert	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received CRL	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ARL	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.

Table 193 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Rcvd data <size> too large! Max size allowed: <max size>	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
Cert trusted: <subject name>	The router has verified the path of the certificate with the listed subject name.
Due to <reason codes>, cert not trusted: <subject name>	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 194 on page 475 for the corresponding descriptions of the codes.

Table 194 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.

Table 194 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 195 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication method.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 196 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.
(D to L)	DMZ to LAN	ACL set for packets traveling from the DMZ to the LAN.
(D to W)	DMZ to WAN	ACL set for packets traveling from the DMZ to the WAN.
(W to D)	WAN to DMZ	ACL set for packets traveling from the WAN to the DMZ.
(L to D)	LAN to DMZ	ACL set for packets traveling from the LAN to the DMZ.
(L to L)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.
(D to D)	DMZ to DMZ/ ZyXEL Device	ACL set for packets traveling from the DMZ to the DMZ or the ZyXEL Device.

Table 197 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 197 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 198 Syslog Logs

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

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

Table 199 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

Table 199 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Log Commands

Go to the command interpreter interface.

Configuring What You Want the ZyXEL Device to Log

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

Figure 271 Displaying Log Categories Example

```

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras>?
Valid commands are:
sys          exit          ether         aux
ip           ipsec         bridge       bm
certificates cnm           8021x        radius
ras>

```

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

Figure 272 Displaying Log Parameters Example

```

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

```

- 4 Use `sys logs category` followed by a log category and a parameter to decide what to record.

Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.

- 5 Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

Displaying Logs

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

Log Command Example

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

```

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

```

#.	time	source	destination	notes
	message			
0	06/08/2004 05:58:21	172.21.4.154	224.0.1.24	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
1	06/08/2004 05:58:20	172.21.3.56	239.255.255.250	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
2	06/08/2004 05:58:20	172.21.0.2	239.255.255.254	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
3	06/08/2004 05:58:20	172.21.3.191	224.0.1.22	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
4	06/08/2004 05:58:20	172.21.0.254	224.0.0.1	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
5	06/08/2004 05:58:20	172.21.4.187:137	172.21.255.255:137	ACCESS
	BLOCK			
	Firewall default policy: UDP (W to W/ZW)			

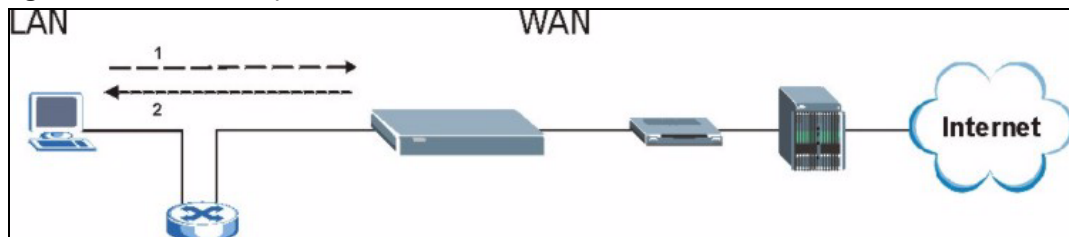
APPENDIX P

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 273 Ideal Setup

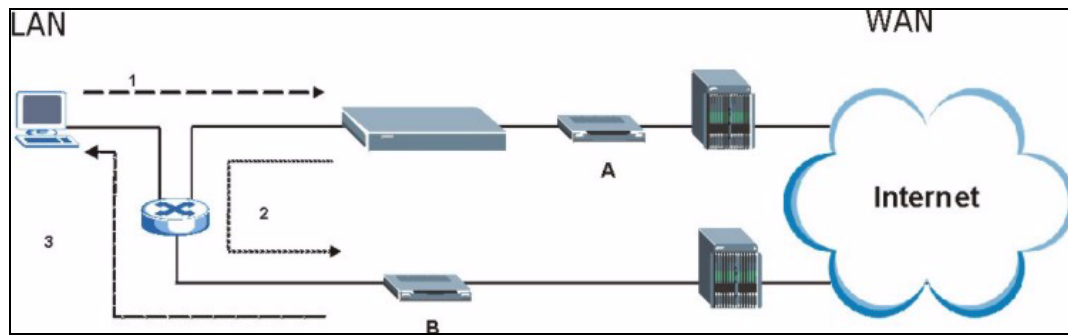


The “Triangle Route” Problem

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 274 “Triangle Route” Problem

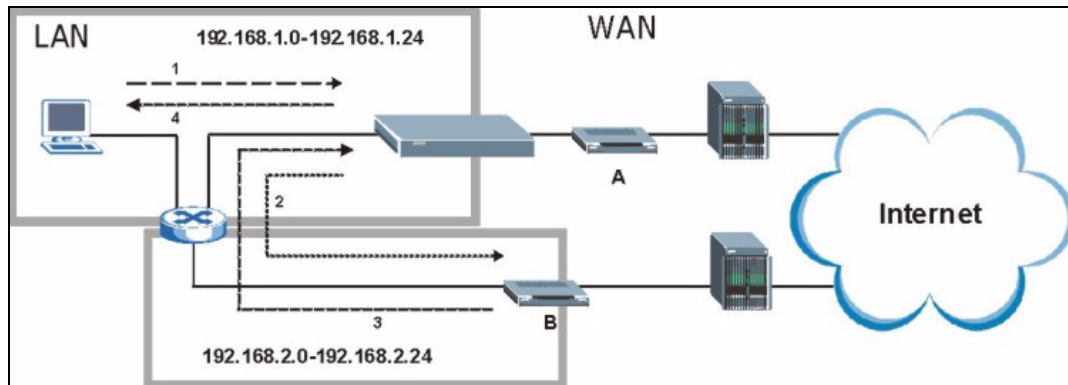
The “Triangle Route” Solutions

This section presents you two solutions to the “triangle route” problem.

IP Aliasing

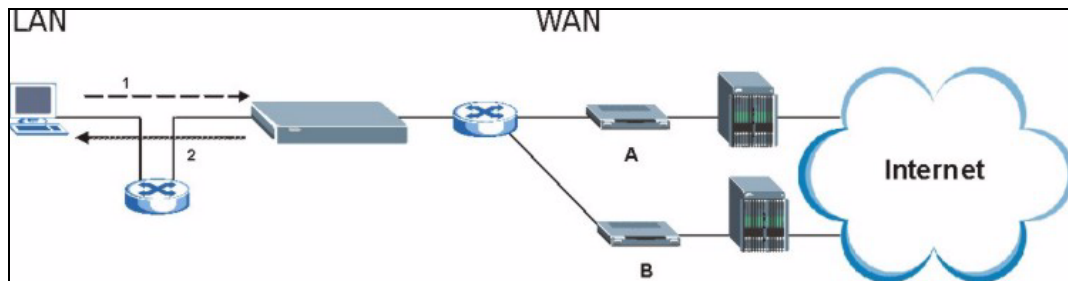
IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyXEL Device supports up to three logical LAN interfaces with the ZyXEL Device being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning 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 the 192.168.2.1 to 192.168.2.24 subnet.
- 3** The reply from WAN goes through the ZyXEL Device to the computer on the LAN in the 192.168.1.1 to 192.168.1.24 subnet.

Figure 275 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 276 Gateways on the WAN Side

Index

A

- Address Assignment [111](#)
- Address Resolution Protocol (ARP) [114](#)
- ADSL standards [42](#)
- Advanced Encryption Standard [405](#)
- AH [235](#)
- AH Protocol [239](#)
- alternative subnet mask notation [391](#)
- antenna gain [134](#)
- Anti-virus
 - Online update [207](#)
 - Registration [207](#)
- Anti-virus packet scan
 - Configuration [205](#)
- Anti-virus scan
 - packet types [205](#)
- Any IP [42](#), [113](#)
 - How it works [114](#)
 - note [114](#)
- Any IP Setup [116](#)
- AP (access point) [399](#)
- applications
 - Internet access [46](#)
- Application-level Firewalls [170](#)
- ATM Adaptation Layer 5 (AAL5) [86](#)
- Attack Alert [200](#)
- Attack Types [174](#)
- Authentication Header [239](#)
- Available Services [220](#)

B

- Backup [347](#)
- Backup Type [101](#)
- Bandwidth Management [293](#)
- Bandwidth Manager Class Configuration [299](#)
- Bandwidth Manager Monitor [302](#)
- Bandwidth Manager Summary [297](#)
- Basic wireless security [76](#)
- Blocking Time [199](#)
- Boot sector virus [203](#)
- Brute-force Attack, [173](#)

BSS [397](#)
BW Budget [299](#)

C

CA [404](#)
CAC [215](#)
CBR (Continuous Bit Rate) [93](#), [98](#)
certificate [251](#)
Certificate Authority [404](#)
change password at login [50](#)
Channel [399](#)
 Interference [399](#)
Channel ID [128](#)
compact [44](#)
compact guide [49](#)
Computer virus [203](#)
Computer virus infection and prevention [204](#)
Computer virus types [203](#)
Configuration [110](#)
Content Access Control
 activation [216](#)
 Administrator Login [231](#)
 Application [215](#)
 configuration steps [215](#)
 Content Filtering Service [217](#)
 create user groups [216](#)
 Customize services [219](#)
 Diagnose [227](#)
 diagnose sequence [227](#)
 Idle Timeout [216](#)
 log out [230](#)
 online status [229](#)
 test web site access privileges [227](#)
 Time Left [229](#)
 Time schedule [217](#)
 Unlimited time schedule [218](#)
 User Account [228](#)
 user accounts [215](#)
 User groups [216](#)
 user groups [215](#)
 User Login [230](#)
 User Profile [228](#)
 Web Site Filters [222](#)
 web site test sequence [227](#)
 WLAN application [215](#)
Content Access Control (CAC) [215](#)
Content Filtering [211](#)
 Categories [211](#)
 Schedule [212](#)
 Trusted computers [213](#)
 URL keyword blocking [211](#)

- Content filtering [211](#)
- content filtering [42](#), [222](#)
- CTS (Clear to Send) [400](#)
- Custom Ports
 - Creating/Editing [191](#)
- Customized Services [190](#)
- Customized services [190](#)

D

- Data Confidentiality [234](#)
- Data Integrity [234](#)
- Data Origin Authentication [234](#)
- Default [349](#)
- default LAN IP address [49](#)
- Denial of Service [170](#), [171](#), [199](#)
- Destination Address [183](#)
- device model number [345](#)
- DH [254](#)
- DHCP [44](#), [110](#), [111](#), [305](#), [333](#)
- DHCP client [44](#)
- DHCP relay [44](#)
- DHCP server [44](#)
- diagnostic [351](#)
- Diffie-Hellman Key Groups [254](#)
- DMZ [151](#), [366](#)
- DNS [317](#)
- DNS Server
 - For VPN Host [245](#)
- Domain Name [111](#), [162](#), [333](#)
- Domain Name System [110](#)
- DoS [171](#)
 - Basics [171](#)
 - Types [172](#)
- DoS (Denial of Service) [42](#), [151](#), [366](#)
- DoS attacks, types of [172](#)
- DSL (Digital Subscriber Line) [369](#)
- DSL line, reinitialize [352](#)
- DSLAM (Digital Subscriber Line Access Multiplexer) [46](#)
- Dynamic DNS [44](#), [305](#)
- dynamic DNS [44](#)
- Dynamic Host Configuration Protocol [44](#)
- Dynamic Secure Gateway Address [241](#)
- Dynamic WEP Key Exchange [404](#)
- DYNDNS Wildcard [305](#)

E

- EAP Authentication [403](#)
- ECHO [162](#)
- E-mail virus [203](#)
- embedded help [53](#)
- Encapsulated Routing Link Protocol (ENET ENCAP) [85](#)
- Encapsulation [85](#), [235](#)
 - ENET ENCAP [85](#)
 - PPP over Ethernet [85](#)
 - PPPoA [86](#)
 - RFC 1483 [86](#)
- Encapsulation Security Payload [239](#)
- Encryption [233](#), [405](#)
- ESP [235](#)
- ESP Protocol [239](#)
- ESS [398](#)
- Ethernet [366](#)
- Extended Service Set [398](#)
- Extended Service Set IDentification [128](#)
- Extended wireless security [75](#)

F

- Fairness-based Scheduler [295](#)
- FCC [4](#)
- FCC Rules [4](#)
- Federal Communications Commission [4](#)
- File infector [203](#)
- Finger [162](#)
- Firewall
 - Access Methods [181](#)
 - Address Type [189](#)
 - Alerts [184](#)
 - Anti-Probing [197](#)
 - Creating/Editing Rules [187](#)
 - Custom Ports [190](#)
 - Enabling [184](#)
 - Firewall Vs Filters [179](#)
 - Guidelines For Enhancing Security [178](#)
 - Introduction [170](#)
 - LAN to WAN Rules [184](#)
 - Policies [181](#)
 - Rule Checklist [182](#)
 - Rule Logic [182](#)
 - Rule Security Ramifications [182](#)
 - Services [195](#)
 - Types [169](#)
 - When To Use [180](#)
- firmware [345](#)
 - upgrade [345](#)

upload [345](#)
upload error [346](#)
Fragmentation Threshold [400](#)
Fragmentation threshold [400](#)
Frame Relay [46](#)
FTP [162](#), [309](#), [312](#)
FTP Restrictions [309](#)
Full Rate [463](#)

G

General Setup [333](#)
General wireless LAN screen [127](#)

H

Half-Open Sessions [199](#)
Hidden node [399](#)
Host [63](#), [334](#), [335](#)
How ZyXEL Device virus scan works [205](#)
HTTP [162](#), [170](#), [171](#), [172](#)
HTTP (Hypertext Transfer Protocol) [345](#)

I

IANA [112](#)
IANA (Internet Assigned Number Authority) [190](#)
IBSS [397](#)
ICMP echo [173](#)
ID Type and Content [245](#)
IEEE 802.11g [45](#), [401](#)
IEEE 802.11i [45](#)
IGMP [113](#)
IKE Phases [252](#)
Independent Basic Service Set [397](#)
initialization vector (IV) [406](#)
Inside Header [236](#)
Install UPnP [323](#)
 Windows Me [323](#)
 Windows XP [325](#)
Integrated Services Digital Network [41](#)
Internal SPTGEN [437](#)
 FTP Upload Example [439](#)
 Points to Remember [437](#)
 Text File [437](#)

- Internet Access [42, 46](#)
- Internet access [65](#)
- Internet Access Setup [354](#)
- Internet access wizard setup [65](#)
- Internet Assigned Numbers AuthoritySee IANA [112](#)
- Internet Control Message Protocol (ICMP) [173, 197](#)
- Internet Key Exchange [252](#)
- Internet Protocol Security [233](#)
- IP Address [111, 162, 163, 164](#)
- IP Address Assignment [87](#)
 - ENET ENCAP [87](#)
 - PPPoA or PPPoE [87](#)
 - RFC 1483 [87](#)
- IP alias [44](#)
- IP Policy Routing (IPPR) [44](#)
- IP Pool [117](#)
- IP Pool Setup [110](#)
- IP protocol type [195](#)
- IP Spoofing [172, 175](#)
- IPSec [233](#)
- IPSec Algorithms [235, 239](#)
- IPSec and NAT [236](#)
- IPSec Architecture [235](#)
- IPSec standard [43](#)
- IPSec VPN Capability [43](#)
- ISDN (Integrated Services Digital Network) [41](#)

K

- Keep Alive [243](#)
- Key Fields For Configuring Rules [183](#)

L

- LAN Setup [85, 109](#)
- LAN TCP/IP [111](#)
- LAN to WAN Rules [184](#)
- LAND [172, 173](#)
- License [3](#)
- Limitations of the ZyXEL Device [205](#)
- Logs [339](#)

M

- MAC Address Filter Action [140](#)

MAC Address Filtering [139](#)
MAC Filter [139](#)
Macro virus [203](#)
Management Information Base (MIB) [314](#)
Manually Update Virus Information [208](#)
Maximize Bandwidth Usage [295](#)
Maximum Burst Size (MBS) [89](#), [94](#), [98](#)
Max-incomplete High [199](#)
Max-incomplete Low [199](#)
Media Bandwidth Management [43](#)
Message Integrity Check (MIC) [405](#)
Metric [88](#)
Multicast [113](#)
Multiplexing [86](#)
multiplexing [86](#)
 LLC-based [86](#)
 VC-based [86](#)
Multiprotocol Encapsulation [86](#)
My IP Address [240](#)

N

Nailed-Up Connection [87](#)
NAT [111](#), [162](#), [163](#)
 Address mapping rule [167](#)
 Application [159](#)
 Definitions [157](#)
 How it works [158](#)
 Mapping Types [159](#)
 What it does [158](#)
 What NAT does [158](#)
NAT (Network Address Translation) [157](#)
NAT mode [161](#)
NAT Traversal [321](#)
NAT traversal [244](#)
navigating the web configurator [52](#)
Negotiation Mode [253](#)
NetBIOS commands [174](#)
Network Address Translation (NAT) [43](#)
Network Management [162](#)
NNTP [162](#)

O

One-Minute High [199](#)
Outside Header [236](#)

P

- Packet Filtering [180](#)
- Packet filtering
 - When to use [180](#)
- Packet Filtering Firewalls [169](#)
- Pairwise Master Key (PMK) [406](#)
- Parental Control [215](#)
- Pattern file [203](#)
- Peak Cell Rate (PCR) [88](#), [94](#), [98](#)
- Perfect Forward Secrecy [254](#)
- PFS [254](#)
- Ping of Death [172](#)
- Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [86](#)
- Point-to-Point [369](#)
- Point-to-Point Tunneling Protocol [162](#)
- POP3 [162](#), [171](#), [172](#)
- PPPoE [85](#)
 - Benefits [85](#)
- PPPoE (Point-to-Point Protocol over Ethernet) [43](#)
- PPTP [162](#)
- Preamble Mode [401](#)
- Pre-defined Web Content Categories [222](#)
- Pre-Shared Key [247](#)
- Priorities [141](#), [297](#)
- Priority [299](#)
- Priority-based Scheduler [294](#)
- protocol type [220](#)

Q

- Quick Start Guide [39](#)

R

- RADIUS [402](#)
 - Shared Secret Key [403](#)
- RADIUS Message Types [402](#)
- RADIUS Messages [402](#)
- reinitialize the ADSL line [352](#)
- Related Documentation [39](#)
- Remote Management and NAT [310](#)
- Remote Management Limitations [309](#)
- Reset button, the [52](#)
- resetting the ZyXEL Device [52](#)
- Restore [348](#)

RF (Radio Frequency) [45](#)
RFC 1483 [86](#)
RFC 1631 [157](#)
RFC2516 [43](#)
RIPSee Routing Information Protocol [112](#)
Routing Information Protocol [112](#)
 Direction [112](#)
 Version [112](#)
RTS (Request To Send) [400](#)
RTS Threshold [399](#), [400](#)
Rules [184](#)
 Checklist [182](#)
 Key Fields [183](#)
 LAN to WAN [184](#)
 Logic [182](#)
 Predefined Services [195](#)

S

SA [233](#)
Safety Warnings [6](#)
Saving the State [175](#)
Scanning engine [203](#)
Scheduler [294](#)
Secure Gateway Address [241](#)
Security Association [233](#)
Security In General [179](#)
Security Parameter Index [257](#)
Security Parameters [407](#)
Security Ramifications [182](#)
Server [159](#), [160](#), [336](#)
Service [183](#)
Service Set [128](#)
Service Type [191](#), [354](#)
Services [162](#)
Signature [203](#)
Signature-based [203](#)
Signature-based virus scan [203](#)
SMTP [162](#)
SMTP Error Messages [343](#)
Smurf [173](#), [174](#)
SNMP [162](#), [313](#)
 Manager [314](#)
 MIBs [314](#)
Source Address [183](#)
SPI [257](#)
Splitters [463](#)
Stateful Inspection [42](#), [169](#), [170](#), [175](#)
 Process [176](#)
 ZyXEL Device [176](#)

Static Route [289](#)
SUA [160](#)
SUA (Single User Account) [160](#)
SUA vs NAT [160](#)
subnet [389](#)
Subnet Mask [111](#), [189](#)
subnet mask [391](#)
subnetting [391](#)
Supporting Disk [39](#)
Sustain Cell Rate (SCR) [94](#), [98](#)
Sustained Cell Rate (SCR) [88](#)
SYN Flood [172](#), [173](#)
SYN-ACK [173](#)
Syntax Conventions [39](#)
Syslog [194](#)
System Name [334](#)
System Parameter Table Generator [437](#)
System Timeout [310](#)

T

TCP Maximum Incomplete [199](#), [200](#)
TCP Security [177](#)
TCP/IP [171](#), [172](#)
Teardrop [172](#)
Telnet [311](#)
Temporal Key Integrity Protocol (TKIP) [405](#)
Text File Format [437](#)
TFTP Restrictions [309](#)
The DeMilitarized Zone (DMZ) [151](#)
Three-Way Handshake [172](#)
Threshold Values [198](#)
Traceroute [175](#)
Traffic Redirect [99](#), [100](#)
Traffic redirect [99](#), [102](#)
traffic redirect [43](#)
Traffic shaping [88](#)
Transport Mode [236](#)
Tunnel Mode [236](#)

U

UBR (Unspecified Bit Rate) [93](#), [98](#)
UDP/ICMP Security [177](#)
Universal Plug and Play [321](#)
 Application [321](#)

Universal Plug and Play (UPnP) [43](#)
Update Schedule [208](#)
Update the virus scan [209](#)
UPnP [321](#)
 Forum [322](#)
 security issues [322](#)
Upper Layer Protocols [177](#), [178](#)
URL keyword blocking [222](#)
User Authentication [406](#)
User Name [306](#)

V

VBR (Variable Bit Rate) [93](#), [98](#)
Viewing Certifications [5](#)
Virtual Channel Identifier (VCI) [86](#)
virtual circuit (VC) [86](#)
Virtual Path Identifier (VPI) [86](#)
Virtual Private Network [43](#), [233](#)
Virus attack [203](#)
Virus life cycle [204](#)
VPI & VCI [86](#)
VPN [233](#)
VPN Applications [234](#)

W

WAN (Wide Area Network) [85](#)
WAN backup [100](#), [102](#)
WAN to LAN Rules [184](#)
Web [310](#)
Web Configurator [49](#), [52](#), [178](#), [183](#)
web configurator screen summary [53](#)
Web Site Filters [222](#)
WEP (Wired Equivalent Privacy) [45](#)
WEP Encryption [131](#)
Wi-Fi Multimedia QoS [141](#)
Wi-Fi Protected Access [405](#)
Wi-Fi Protected Access (WPA) [45](#)
Wireless LAN MAC Address Filtering [45](#)
WLAN
 Interference [399](#)
 Security parameters [407](#)
Worm [203](#)
WPA [405](#)
WPA2 [405](#)
WPA2-Pre-Shared Key [405](#)

WPA2-PSK [405](#)

WPA-PSK [405](#)

Z

Zero Configuration Internet Access [42](#)

Zero configuration Internet access [90](#)

ZyXEL Device anti-virus packet scan [204](#)

ZyXEL_s Firewall
Introduction [170](#)