

# *NBG410W3G Series*

*3G Wireless Router*

## *User's Guide*

Version 4.03  
08/2008  
Edition 1

**DRAFT**

---

**ZyXEL**  
[www.zyxel.com](http://www.zyxel.com)



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide  
The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help  
Embedded web help for descriptions of individual screens and supplementary information.
- Supporting Disk  
Refer to the included CD for support documents.
- ZyXEL Web Site  
Please refer to [www.zyxel.com](http://www.zyxel.com) for additional support documentation and product certifications.

## User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,  
ZyXEL Communications Corp.,  
6 Innovation Road II,  
Science-Based Industrial Park,  
Hsinchu, 300, Taiwan.

E-mail: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this User's Guide.



---

Warnings tell you about things that could harm you or your device.

---



---

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.










---

## Syntax Conventions

- The NBG410W3G and NBG412W3G may be referred to as the “ZyXEL Device”, the “device”, the “system”, or the “NBG410W3G Series” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

**Icons Used in Figures**

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

# Safety Warnings



---

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

---

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.







# Contents Overview

<b>Introduction .....</b>	<b>33</b>
Getting to Know Your ZyXEL Device .....	35
Introducing the Web Configurator .....	43
Wizard Setup .....	59
Tutorials .....	65
<b>Network .....</b>	<b>99</b>
LAN Screens .....	101
WAN Screens .....	111
DMZ Screens .....	135
<b>Wireless .....</b>	<b>145</b>
Wi-Fi .....	147
<b>Security .....</b>	<b>165</b>
Firewall .....	167
Authentication Server .....	191
Certificates .....	195
<b>Advanced .....</b>	<b>223</b>
Network Address Translation (NAT) .....	225
Static Route .....	243
DNS .....	247
Remote Management .....	259
UPnP .....	281
Custom Application .....	291
ALG Screen .....	293
<b>Logs and Maintenance .....</b>	<b>299</b>
Logs Screens .....	301
Maintenance .....	325
<b>Troubleshooting and Specifications .....</b>	<b>337</b>
Troubleshooting .....	339
Product Specifications .....	345
<b>Appendices and Index .....</b>	<b>351</b>



# Table of Contents

<b>About This User's Guide</b> .....	<b>3</b>
<b>Document Conventions</b> .....	<b>4</b>
<b>Safety Warnings</b> .....	<b>6</b>
<b>Contents Overview</b> .....	<b>9</b>
<b>Table of Contents</b> .....	<b>11</b>
<b>List of Figures</b> .....	<b>21</b>
<b>List of Tables</b> .....	<b>29</b>
<b>Part I: Introduction</b> .....	<b>33</b>
<b>Chapter 1</b>	
<b>Getting to Know Your ZyXEL Device</b> .....	<b>35</b>
1.1 Overview .....	35
1.2 Applications for the ZyXEL Device .....	35
1.2.1 3G WAN Application .....	35
1.2.2 Secure Broadband Internet Access via Cable or DSL Modem .....	36
1.3 Ways to Manage the ZyXEL Device .....	36
1.4 Configuring Your ZyXEL Device's Security Features .....	37
1.4.1 Control Access to Your Device .....	37
1.4.2 Wireless Security .....	37
1.4.3 Firewall .....	37
1.4.4 NAT .....	38
1.4.5 UPnP .....	38
1.5 Maintaining Your ZyXEL Device .....	38
1.5.1 Front Panel Lights .....	39
<b>Chapter 2</b>	
<b>Introducing the Web Configurator</b> .....	<b>43</b>
2.1 Web Configurator Overview .....	43
2.2 Accessing the ZyXEL Device Web Configurator .....	43
2.3 Resetting the ZyXEL Device .....	45
2.3.1 Procedure To Use The Reset Button .....	45
2.3.2 Uploading a Configuration File Via Console Port .....	45

2.4 Navigating the ZyXEL Device Web Configurator .....	46
2.4.1 Title Bar .....	46
2.4.2 Main Window .....	47
2.4.3 HOME Screen .....	47
2.4.4 Navigation Panel .....	52
2.4.5 Port Statistics .....	54
2.4.6 Show Statistics: Line Chart .....	55
2.4.7 DHCP Table Screen .....	56
<b>Chapter 3</b>	
<b>Wizard Setup .....</b>	<b>59</b>
3.1 Wizard Setup Overview .....	59
3.2 Internet Access .....	59
3.2.1 ISP Parameters .....	59
3.2.2 Internet Access Wizard Setup Complete .....	64
<b>Chapter 4</b>	
<b>Tutorials .....</b>	<b>65</b>
4.1 DMZ Overview .....	65
4.2 DMZ Setup Example .....	66
4.2.1 Basic Setup .....	66
4.2.2 Advanced Setup .....	68
4.3 Firewall Rule Setup .....	69
4.4 Setting Up a VoIP Phone with H.323 .....	72
4.5 Using NAT with Multiple Public IP Addresses .....	77
4.5.1 Example Parameters and Scenario .....	77
4.5.2 Configuring the WAN Connection with a Static IP Address .....	78
4.5.3 Public IP Address Mapping .....	82
4.5.4 Forwarding Traffic from the WAN to a Local Computer .....	87
4.5.5 Allow WAN-to-LAN Traffic through the Firewall .....	89
4.5.6 Testing the Connections .....	96
4.6 Using NAT with Multiple Game Players .....	96
<b>Part II: Network .....</b>	<b>99</b>
<b>Chapter 5</b>	
<b>LAN Screens .....</b>	<b>101</b>
5.1 LAN, WAN and the ZyXEL Device .....	101
5.2 IP Address and Subnet Mask .....	101
5.2.1 Private IP Addresses .....	102
5.3 DHCP .....	102

5.3.1 IP Pool Setup .....	103
5.4 RIP Setup .....	103
5.5 Multicast .....	103
5.6 WINS .....	104
5.7 LAN .....	104
5.8 LAN Static DHCP .....	106
5.9 LAN IP Alias .....	107
5.10 LAN Port Roles .....	109
<b>Chapter 6</b>	
<b>WAN Screens.....</b>	<b>111</b>
6.1 WAN Overview .....	111
6.2 Multiple WAN .....	111
6.3 TCP/IP Priority (Metric) .....	112
6.4 WAN General .....	112
6.5 WAN IP Address Assignment .....	115
6.6 DNS Server Address Assignment .....	116
6.7 WAN MAC Address .....	116
6.8 WAN 1 .....	117
6.8.1 WAN Ethernet Encapsulation .....	117
6.8.2 PPPoE Encapsulation .....	120
6.8.3 PPTP Encapsulation .....	123
6.9 3G (WAN 2) .....	126
6.10 Traffic Redirect .....	132
6.11 Configuring Traffic Redirect .....	133
<b>Chapter 7</b>	
<b>DMZ Screens.....</b>	<b>135</b>
7.1 DMZ .....	135
7.2 Configuring DMZ .....	135
7.3 DMZ Static DHCP .....	138
7.4 DMZ IP Alias .....	139
7.5 DMZ Public IP Address Example .....	141
7.6 DMZ Private and Public IP Address Example .....	141
7.7 DMZ Port Roles .....	142
<b>Part III: Wireless.....</b>	<b>145</b>
<b>Chapter 8</b>	
<b>Wi-Fi.....</b>	<b>147</b>
8.1 Wi-Fi Introduction .....	147

8.2 Wireless Security Overview .....	148
8.2.1 SSID .....	148
8.2.2 MAC Address Filter .....	148
8.2.3 User Authentication .....	149
8.2.4 Encryption .....	149
8.2.5 Additional Installation Requirements for Using 802.1x .....	151
8.3 Wireless Card .....	151
8.3.1 SSID Profile .....	153
8.4 Configuring Wireless Security .....	154
8.4.1 No Security .....	156
8.4.2 Static WEP .....	156
8.4.3 IEEE 802.1x Only .....	157
8.4.4 IEEE 802.1x + Static WEP .....	158
8.4.5 WPA, WPA2, WPA2-MIX .....	160
8.4.6 WPA-PSK, WPA2-PSK, WPA2-PSK-MIX .....	161
8.5 MAC Filter .....	162
<b>Part IV: Security .....</b>	<b>165</b>
<b>Chapter 9</b>	
<b>Firewall.....</b>	<b>167</b>
9.1 Firewall Overview .....	167
9.2 Packet Direction Matrix .....	168
9.3 Packet Direction Examples .....	169
9.4 Security Considerations .....	170
9.5 Firewall Rules Example .....	171
9.6 Asymmetrical Routes .....	173
9.6.1 Asymmetrical Routes and IP Alias .....	173
9.7 Firewall Default Rule .....	173
9.8 Firewall Rule Summary .....	175
9.8.1 Firewall Edit Rule .....	177
9.9 Anti-Probing .....	180
9.10 Firewall Thresholds .....	181
9.10.1 Threshold Values .....	182
9.11 Threshold Screen .....	182
9.12 Service .....	184
9.12.1 Firewall Edit Custom Service .....	185
9.13 My Service Firewall Rule Example .....	186
<b>Chapter 10</b>	
<b>Authentication Server.....</b>	<b>191</b>

10.1 Authentication Server Overview .....	191
10.2 Local User Database .....	191
10.3 RADIUS .....	193
<b>Chapter 11</b>	
<b>Certificates .....</b>	<b>195</b>
11.1 Certificates Overview .....	195
11.1.1 Advantages of Certificates .....	196
11.2 Self-signed Certificates .....	196
11.3 Verifying a Certificate .....	196
11.3.1 Checking the Fingerprint of a Certificate on Your Computer .....	196
11.4 Configuration Summary .....	197
11.5 My Certificates .....	198
11.6 My Certificate Details .....	200
11.7 My Certificate Export .....	202
11.7.1 Certificate File Export Formats .....	202
11.8 My Certificate Import .....	203
11.8.1 Certificate File Formats .....	203
11.9 My Certificate Create .....	205
11.10 Trusted CAs .....	209
11.11 Trusted CA Details .....	211
11.12 Trusted CA Import .....	214
11.13 Trusted Remote Hosts .....	215
11.14 Trusted Remote Hosts Import .....	217
11.15 Trusted Remote Host Certificate Details .....	218
11.16 Directory Servers .....	220
11.17 Directory Server Add or Edit .....	221
<b>Part V: Advanced .....</b>	<b>223</b>
<b>Chapter 12</b>	
<b>Network Address Translation (NAT).....</b>	<b>225</b>
12.1 NAT Overview .....	225
12.1.1 NAT Definitions .....	225
12.1.2 What NAT Does .....	226
12.1.3 How NAT Works .....	226
12.1.4 NAT Application .....	227
12.1.5 Port Restricted Cone NAT .....	228
12.1.6 NAT Mapping Types .....	229
12.2 Using NAT .....	230
12.2.1 SUA (Single User Account) Versus NAT .....	230

12.3 NAT Overview Screen .....	230
12.4 NAT Address Mapping .....	232
12.4.1 What NAT Does .....	232
12.4.2 NAT Address Mapping Edit .....	234
12.5 Port Forwarding .....	235
12.5.1 Default Server IP Address .....	235
12.5.2 Port Forwarding: Services and Port Numbers .....	236
12.5.3 Configuring Servers Behind Port Forwarding (Example) .....	236
12.5.4 NAT and Multiple WAN .....	237
12.5.5 Port Translation .....	237
12.6 Port Forwarding Screen .....	238
12.7 Port Triggering .....	240
<b>Chapter 13</b>	
<b>Static Route .....</b>	<b>243</b>
13.1 IP Static Route .....	243
13.2 IP Static Route .....	244
13.2.1 IP Static Route Edit .....	245
<b>Chapter 14</b>	
<b>DNS .....</b>	<b>247</b>
14.1 DNS Overview .....	247
14.2 DNS Server Address Assignment .....	247
14.3 DNS Servers .....	247
14.4 Address Record .....	248
14.4.1 DNS Wildcard .....	248
14.5 Name Server Record .....	248
14.5.1 Private DNS Server .....	248
14.6 System Screen .....	248
14.6.1 Adding an Address Record .....	250
14.6.2 Inserting a Name Server Record .....	251
14.7 DNS Cache .....	252
14.8 Configure DNS Cache .....	252
14.9 Configuring DNS DHCP .....	254
14.10 Dynamic DNS .....	255
14.10.1 DYNDNS Wildcard .....	255
14.10.2 High Availability .....	256
14.11 Configuring Dynamic DNS .....	256
<b>Chapter 15</b>	
<b>Remote Management.....</b>	<b>259</b>
15.1 Remote Management Overview .....	259
15.1.1 Remote Management Limitations .....	260



---

15.1.2 System Timeout .....	260
15.2 WWW (HTTP and HTTPS) .....	260
15.3 WWW .....	261
15.4 HTTPS Example .....	263
15.4.1 Internet Explorer Warning Messages .....	263
15.4.2 Netscape Navigator Warning Messages .....	263
15.4.3 Avoiding the Browser Warning Messages .....	264
15.4.4 Login Screen .....	265
15.5 SSH .....	267
15.6 How SSH Works .....	267
15.7 SSH Implementation on the ZyXEL Device .....	268
15.7.1 Requirements for Using SSH .....	268
15.8 Configuring SSH .....	269
15.9 Secure Telnet Using SSH Examples .....	270
15.9.1 Example 1: Microsoft Windows .....	270
15.9.2 Example 2: Linux .....	270
15.10 Secure FTP Using SSH Example .....	271
15.11 Telnet .....	272
15.12 Configuring TELNET .....	272
15.13 FTP .....	273
15.14 SNMP .....	274
15.14.1 Supported MIBs .....	275
15.14.2 SNMP Traps .....	276
15.14.3 REMOTE MANAGEMENT: SNMP .....	276
15.15 DNS .....	277
15.16 Introducing Vantage CNM .....	278
15.17 Configuring CNM .....	278
15.17.1 Additional Configuration for Vantage CNM .....	280
<b>Chapter 16</b>	
<b>UPnP .....</b>	<b>281</b>
16.1 Universal Plug and Play Overview .....	281
16.1.1 How Do I Know If I'm Using UPnP? .....	281
16.1.2 NAT Traversal .....	281
16.1.3 Cautions with UPnP .....	281
16.1.4 UPnP and ZyXEL .....	282
16.2 Configuring UPnP .....	282
16.3 Displaying UPnP Port Mapping .....	283
16.4 Installing UPnP in Windows Example .....	284
16.4.1 Installing UPnP in Windows Me .....	285
16.4.2 Installing UPnP in Windows XP .....	286
16.5 Using UPnP in Windows XP Example .....	286
16.5.1 Auto-discover Your UPnP-enabled Network Device .....	287

16.5.2 Web Configurator Easy Access .....	288
<b>Chapter 17</b>	
<b>Custom Application .....</b>	<b>291</b>
17.1 Custom Application .....	291
17.2 Custom Application Configuration .....	291
<b>Chapter 18</b>	
<b>ALG Screen .....</b>	<b>293</b>
18.1 ALG Introduction .....	293
18.1.1 ALG and NAT .....	293
18.1.2 ALG and the Firewall .....	293
18.1.3 ALG and Multiple WAN .....	294
18.2 FTP .....	294
18.3 H.323 .....	294
18.4 RTP .....	294
18.4.1 H.323 ALG Details .....	294
18.5 SIP .....	295
18.5.1 STUN .....	295
18.5.2 SIP ALG Details .....	296
18.5.3 SIP Signaling Session Timeout .....	296
18.5.4 SIP Audio Session Timeout .....	296
18.6 ALG Screen .....	296
<b>Part VI: Logs and Maintenance.....</b>	<b>299</b>
<b>Chapter 19</b>	
<b>Logs Screens .....</b>	<b>301</b>
19.1 Configuring View Log .....	301
19.2 Log Description Example .....	302
19.2.1 About the Certificate Not Trusted Log .....	303
19.3 Configuring Log Settings .....	304
19.4 Configuring Reports .....	307
19.4.1 Viewing Web Site Hits .....	309
19.4.2 Viewing Host IP Address .....	309
19.4.3 Viewing Protocol/Port .....	310
19.4.4 System Reports Specifications .....	312
19.5 Log Descriptions .....	312
19.6 Syslog Logs .....	323
<b>Chapter 20</b>	
<b>Maintenance .....</b>	<b>325</b>

20.1 Maintenance Overview .....	325
20.2 General Setup and System Name .....	325
20.2.1 General Setup .....	325
20.3 Configuring Password .....	326
20.4 Time and Date .....	327
20.5 Pre-defined NTP Time Server Pools .....	330
20.5.1 Resetting the Time .....	330
20.5.2 Time Server Synchronization .....	330
20.6 F/W Upload Screen .....	331
20.7 Backup and Restore .....	333
20.7.1 Backup Configuration .....	334
20.7.2 Restore Configuration .....	334
20.7.3 Back to Factory Defaults .....	335
20.8 Restart Screen .....	336
<b>Part VII: Troubleshooting and Specifications .....</b>	<b>337</b>
<b>Chapter 21</b>	
<b>Troubleshooting.....</b>	<b>339</b>
21.1 Power, Hardware Connections, and LEDs .....	339
21.2 ZyXEL Device Access and Login .....	340
21.3 Internet Access .....	342
21.4 3G Connection .....	343
<b>Chapter 22</b>	
<b>Product Specifications .....</b>	<b>345</b>
22.1 General ZyXEL Device Specifications .....	345
22.2 Wall-mounting Instructions .....	347
22.3 Power Adaptor Specifications .....	349
<b>Part VIII: Appendices and Index .....</b>	<b>351</b>
Appendix A Pop-up Windows, JavaScripts and Java Permissions .....	353
Appendix B Setting up Your Computer's IP Address.....	361
Appendix C IP Addresses and Subnetting .....	377
Appendix D Common Services .....	385
Appendix E Wireless LANs .....	389

Table of Contents

---

Appendix F Importing Certificates .....	403
Appendix G Legal Information .....	415
Appendix H Customer Support.....	419
<b>Index.....</b>	<b>425</b>

# List of Figures

Figure 1 3G WAN Application .....	36
Figure 2 Secure Internet Access via Cable or DSL Modem .....	36
Figure 3 Front Panel .....	39
Figure 4 Login Screen .....	44
Figure 5 Change Password Screen .....	44
Figure 6 Replace Certificate Screen .....	44
Figure 7 Example Xmodem Upload .....	46
Figure 8 HOME Screen .....	46
Figure 9 Web Configurator HOME Screen .....	47
Figure 10 HOME > Show Statistics .....	55
Figure 11 HOME > Show Statistics > Line Chart .....	56
Figure 12 HOME > DHCP Table .....	57
Figure 13 Wizard Setup Welcome .....	59
Figure 14 ISP Parameters: Ethernet Encapsulation .....	60
Figure 15 ISP Parameters: PPPoE Encapsulation .....	61
Figure 16 ISP Parameters: PPTP Encapsulation .....	63
Figure 17 Internet Access Setup Complete .....	64
Figure 18 DMZ Overview .....	65
Figure 19 DMZ Tutorial: DMZ Setup .....	66
Figure 20 DMZ Tutorial: NETWORK > DMZ > Static DHCP .....	67
Figure 21 DMZ Tutorial: NETWORK > DMZ .....	67
Figure 22 DMZ Tutorial: ADVANCED > NAT Overview .....	68
Figure 23 DMZ Tutorial: ADVANCED > ALG .....	68
Figure 24 DMZ Tutorial: ADVANCED > NAT > Port Forwarding .....	69
Figure 25 DMZ Tutorial: SECURITY > Firewall > Rule Summary .....	70
Figure 26 DMZ Tutorial: NETWORK > Firewall > Rule Summary: Firewall - Edit .....	71
Figure 27 DMZ Tutorial: SECURITY > Firewall > Rule Summary Example .....	72
Figure 28 Tutorial: H.323 Phone Setup .....	72
Figure 29 H.323 Tutorial: NETWORK > LAN > Static DHCP .....	73
Figure 30 H.323 Tutorial: ADVANCED > ALG .....	73
Figure 31 H.323 Tutorial: ADVANCED > NAT > Port Forwarding .....	74
Figure 32 H.323 Tutorial: SECURITY > Firewall > Rule Summary .....	74
Figure 33 H.323 Tutorial: SECURITY > Firewall > Rule Summary .....	76
Figure 34 H.323 Tutorial: SECURITY > Firewall > Rule Summary .....	77
Figure 35 Tutorial Example: Using NAT with Static Public IP Addresses .....	78
Figure 36 Tutorial Example: WAN Connection with a Static Public IP Address .....	79
Figure 37 Tutorial Example: WAN 1 Screen .....	79
Figure 38 Tutorial Example: DNS > System .....	80

Figure 39 Tutorial Example: DNS > System Edit-1 .....	80
Figure 40 Tutorial Example: DNS > System Edit-2 .....	81
Figure 41 Tutorial Example: DNS > System: Done .....	81
Figure 42 Tutorial Example: Status .....	82
Figure 43 Tutorial Example: Mapping Multiple Public IP Addresses to Inside Servers .....	83
Figure 44 Tutorial Example: NAT > NAT Overview .....	84
Figure 45 Tutorial Example: NAT > Address Mapping .....	85
Figure 46 Tutorial Example: NAT Address Mapping Edit: One-to-One (1) .....	85
Figure 47 Tutorial Example: NAT Address Mapping Edit: One-to-One (2) .....	86
Figure 48 Tutorial Example: NAT Address Mapping Edit: Many-to-One .....	86
Figure 49 Tutorial Example: NAT Address Mapping Done .....	87
Figure 50 Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer .....	88
Figure 51 Tutorial Example: NAT Address Mapping Edit: Server .....	88
Figure 52 Tutorial Example: NAT Port Forwarding .....	89
Figure 53 Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer .....	89
Figure 54 Tutorial Example: Firewall Default Rule .....	90
Figure 55 Tutorial Example: Firewall Rule: WAN1 to LAN .....	90
Figure 56 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Web Server .....	91
Figure 57 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Web Server .....	92
Figure 58 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Mail Server .....	93
Figure 59 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Mail Server .....	93
Figure 60 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for FTP Server .....	94
Figure 61 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for FTP Server .....	95
Figure 62 Tutorial Example: Firewall Rule Summary .....	95
Figure 63 Tutorial Example: NAT Address Mapping Done: Game Playing .....	97
Figure 64 LAN and WAN .....	101
Figure 65 NETWORK > LAN .....	104
Figure 66 NETWORK > LAN > Static DHCP .....	107
Figure 67 Physical Network & Partitioned Logical Networks .....	108
Figure 68 NETWORK > LAN > IP Alias .....	108
Figure 69 NETWORK > LAN > Port Roles .....	110
Figure 70 Port Roles Change Complete .....	110
Figure 71 NETWORK > WAN General .....	113
Figure 72 NETWORK > WAN > WAN 1 (Ethernet Encapsulation) .....	117
Figure 73 NETWORK > WAN > WAN 1 (PPPoE Encapsulation) .....	121
Figure 74 NETWORK > WAN > WAN 1 (PPTP Encapsulation) .....	124
Figure 75 NETWORK > WAN > 3G (WAN 2) .....	128
Figure 76 Traffic Redirect WAN Setup .....	132
Figure 77 Traffic Redirect LAN Setup .....	132
Figure 78 NETWORK > WAN > Traffic Redirect .....	133
Figure 79 NETWORK > DMZ .....	136
Figure 80 NETWORK > DMZ > Static DHCP .....	138
Figure 81 NETWORK > DMZ > IP Alias .....	140

Figure 82 DMZ Public Address Example .....	141
Figure 83 DMZ Private and Public Address Example .....	142
Figure 84 NETWORK > DMZ > Port Roles .....	143
Figure 85 Example of a Wireless Network .....	147
Figure 86 WIRELESS > Wi-Fi > Wireless Card .....	151
Figure 87 WIRELESS > Wi-Fi > Configuring SSID .....	154
Figure 88 WIRELESS > Wi-Fi > Security .....	155
Figure 89 WIRELESS > Wi-Fi > Security: None .....	156
Figure 90 WIRELESS > Wi-Fi > Security: WEP .....	157
Figure 91 WIRELESS > Wi-Fi > Security: 802.1x Only .....	158
Figure 92 WIRELESS > Wi-Fi > Security: 802.1x + Static WEP .....	159
Figure 93 WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX .....	160
Figure 94 WIRELESS > Wi-Fi > Security: WPA(2)-PSK .....	161
Figure 95 WIRELESS > Wi-Fi > MAC Filter .....	163
Figure 96 Default Firewall Action .....	167
Figure 97 SECURITY > FIREWALL > Default Rule .....	168
Figure 98 Default Block Traffic From WAN1 to DMZ Example .....	169
Figure 99 Blocking All LAN to WAN IRC Traffic Example .....	171
Figure 100 Limited LAN to WAN IRC Traffic Example .....	172
Figure 101 Using IP Alias to Solve the Triangle Route Problem .....	173
Figure 102 SECURITY > FIREWALL > Default Rule .....	174
Figure 103 SECURITY > FIREWALL > Rule Summary .....	176
Figure 104 SECURITY > FIREWALL > Rule Summary > Edit .....	178
Figure 105 SECURITY > FIREWALL > Anti-Probing .....	180
Figure 106 Three-Way Handshake .....	181
Figure 107 SECURITY > FIREWALL > Threshold .....	182
Figure 108 SECURITY > FIREWALL > Service .....	184
Figure 109 Firewall Edit Custom Service .....	185
Figure 110 My Service Firewall Rule Example: Service .....	186
Figure 111 My Service Firewall Rule Example: Edit Custom Service .....	187
Figure 112 My Service Firewall Rule Example: Rule Summary .....	187
Figure 113 My Service Firewall Rule Example: Rule Edit: Source and Destination Addresses .....	188
Figure 114 My Service Firewall Rule Example: Edit Rule: Service Configuration .....	189
Figure 115 My Service Firewall Rule Example: Rule Summary: Completed .....	190
Figure 116 SECURITY > AUTH SERVER > Local User Database .....	192
Figure 117 SECURITY > AUTH SERVER > RADIUS .....	193
Figure 118 Certificates on Your Computer .....	196
Figure 119 Certificate Details .....	197
Figure 120 Certificate Configuration Overview .....	197
Figure 121 SECURITY > CERTIFICATES > My Certificates .....	198
Figure 122 SECURITY > CERTIFICATES > My Certificates > Details .....	200
Figure 123 SECURITY > CERTIFICATES > My Certificates > Export .....	202
Figure 124 SECURITY > CERTIFICATES > My Certificates > Import .....	204

Figure 125 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12 .....	204
Figure 126 SECURITY > CERTIFICATES > My Certificates > Create (Basic) .....	205
Figure 127 SECURITY > CERTIFICATES > My Certificates > Create (Advanced) .....	206
Figure 128 SECURITY > CERTIFICATES > Trusted CAs .....	210
Figure 129 SECURITY > CERTIFICATES > Trusted CAs > Details .....	212
Figure 130 SECURITY > CERTIFICATES > Trusted CAs > Import .....	215
Figure 131 SECURITY > CERTIFICATES > Trusted Remote Hosts .....	216
Figure 132 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import .....	217
Figure 133 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details .....	218
Figure 134 SECURITY > CERTIFICATES > Directory Servers .....	220
Figure 135 SECURITY > CERTIFICATES > Directory Server > Add .....	221
Figure 136 How NAT Works .....	227
Figure 137 NAT Application With IP Alias .....	228
Figure 138 Port Restricted Cone NAT Example .....	229
Figure 139 ADVANCED > NAT > NAT Overview .....	231
Figure 140 ADVANCED > NAT > Address Mapping .....	233
Figure 141 ADVANCED > NAT > Address Mapping > Edit .....	234
Figure 142 Multiple Servers Behind NAT Example .....	237
Figure 143 Port Translation Example .....	238
Figure 144 ADVANCED > NAT > Port Forwarding .....	239
Figure 145 Trigger Port Forwarding Process: Example .....	240
Figure 146 ADVANCED > NAT > Port Triggering .....	241
Figure 147 Example of Static Routing Topology .....	243
Figure 148 ADVANCED > STATIC ROUTE > IP Static Route .....	244
Figure 149 ADVANCED > STATIC ROUTE > IP Static Route > Edit .....	245
Figure 150 ADVANCED > DNS > System DNS .....	249
Figure 151 ADVANCED > DNS > Add (Address Record) .....	250
Figure 152 ADVANCED > DNS > Insert (Name Server Record) .....	251
Figure 153 ADVANCED > DNS > Cache .....	253
Figure 154 ADVANCED > DNS > DHCP .....	254
Figure 155 ADVANCED > DNS > DDNS .....	256
Figure 156 Secure and Insecure Remote Management From the WAN .....	259
Figure 157 HTTPS Implementation .....	261
Figure 158 ADVANCED > REMOTE MGMT > WWW .....	262
Figure 159 Security Alert Dialog Box (Internet Explorer) .....	263
Figure 160 Security Certificate 1 (Netscape) .....	264
Figure 161 Security Certificate 2 (Netscape) .....	264
Figure 162 Example: Lock Denoting a Secure Connection .....	265
Figure 163 Replace Certificate .....	266
Figure 164 Device-specific Certificate .....	266
Figure 165 Common ZyXEL Device Certificate .....	267
Figure 166 SSH Communication Over the WAN Example .....	267
Figure 167 How SSH Works .....	268



---

Figure 168 ADVANCED > REMOTE MGMT > SSH .....	269
Figure 169 SSH Example 1: Store Host Key .....	270
Figure 170 SSH Example 2: Test .....	270
Figure 171 SSH Example 2: Log in .....	271
Figure 172 Secure FTP: Firmware Upload Example .....	272
Figure 173 ADVANCED > REMOTE MGMT > Telnet .....	272
Figure 174 ADVANCED > REMOTE MGMT > FTP .....	273
Figure 175 SNMP Management Model .....	275
Figure 176 ADVANCED > REMOTE MGMT > SNMP .....	276
Figure 177 ADVANCED > REMOTE MGMT > DNS .....	278
Figure 178 ADVANCED > REMOTE MGMT > CNM .....	279
Figure 179 ADVANCED > UPnP .....	282
Figure 180 ADVANCED > UPnP > Ports .....	283
Figure 181 ADVANCED > Custom APP .....	292
Figure 182 H.323 ALG Example .....	295
Figure 183 H.323 with Multiple WAN IP Addresses .....	295
Figure 184 SIP ALG Example .....	296
Figure 185 ADVANCED > ALG .....	297
Figure 186 LOGS > View Log .....	301
Figure 187 myZyXEL.com: Download Center .....	303
Figure 188 myZyXEL.com: Certificate Download .....	304
Figure 189 LOGS > Log Settings .....	305
Figure 190 LOGS > Reports .....	308
Figure 191 LOGS > Reports: Web Site Hits Example .....	309
Figure 192 LOGS > Reports: Host IP Address Example .....	310
Figure 193 LOGS > Reports: Protocol/Port Example .....	311
Figure 194 MAINTENANCE > General Setup .....	326
Figure 195 MAINTENANCE > Password .....	327
Figure 196 MAINTENANCE > Time and Date .....	328
Figure 197 Synchronization in Process .....	330
Figure 198 Synchronization is Successful .....	331
Figure 199 Synchronization Fail .....	331
Figure 200 MAINTENANCE > Firmware Upload .....	332
Figure 201 Firmware Upload In Process .....	332
Figure 202 Network Temporarily Disconnected .....	333
Figure 203 Firmware Upload Error .....	333
Figure 204 MAINTENANCE > Backup and Restore .....	334
Figure 205 Configuration Upload Successful .....	335
Figure 206 Network Temporarily Disconnected .....	335
Figure 207 Configuration Upload Error .....	335
Figure 208 Reset Warning Message .....	336
Figure 209 MAINTENANCE > Restart .....	336
Figure 210 Wall-mounting Example .....	348

Figure 211 Masonry Plug and M4 Tap Screw .....	348
Figure 212 Pop-up Blocker .....	353
Figure 213 Internet Options: Privacy .....	354
Figure 214 Internet Options: Privacy .....	355
Figure 215 Pop-up Blocker Settings .....	355
Figure 216 Internet Options: Security .....	356
Figure 217 Security Settings - Java Scripting .....	357
Figure 218 Security Settings - Java .....	357
Figure 219 Java (Sun) .....	358
Figure 220 Mozilla Firefox: Tools > Options .....	359
Figure 221 Mozilla Firefox Content Security .....	359
Figure 222 WInows 95/98/Me: Network: Configuration .....	362
Figure 223 Windows 95/98/Me: TCP/IP Properties: IP Address .....	363
Figure 224 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	364
Figure 225 Windows XP: Start Menu .....	365
Figure 226 Windows XP: Control Panel .....	365
Figure 227 Windows XP: Control Panel: Network Connections: Properties .....	366
Figure 228 Windows XP: Local Area Connection Properties .....	366
Figure 229 Windows XP: Internet Protocol (TCP/IP) Properties .....	367
Figure 230 Windows XP: Advanced TCP/IP Properties .....	368
Figure 231 Windows XP: Internet Protocol (TCP/IP) Properties .....	369
Figure 232 Macintosh OS 8/9: Apple Menu .....	370
Figure 233 Macintosh OS 8/9: TCP/IP .....	370
Figure 234 Macintosh OS X: Apple Menu .....	371
Figure 235 Macintosh OS X: Network .....	372
Figure 236 Red Hat 9.0: KDE: Network Configuration: Devices .....	373
Figure 237 Red Hat 9.0: KDE: Ethernet Device: General .....	373
Figure 238 Red Hat 9.0: KDE: Network Configuration: DNS .....	374
Figure 239 Red Hat 9.0: KDE: Network Configuration: Activate .....	374
Figure 240 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .....	375
Figure 241 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .....	375
Figure 242 Red Hat 9.0: DNS Settings in resolv.conf .....	375
Figure 243 Red Hat 9.0: Restart Ethernet Card .....	375
Figure 244 Red Hat 9.0: Checking TCP/IP Properties .....	376
Figure 245 Network Number and Host ID .....	378
Figure 246 Subnetting Example: Before Subnetting .....	380
Figure 247 Subnetting Example: After Subnetting .....	381
Figure 248 Peer-to-Peer Communication in an Ad-hoc Network .....	389
Figure 249 Basic Service Set .....	390
Figure 250 Infrastructure WLAN .....	391
Figure 251 RTS/CTS .....	392
Figure 252 WPA(2) with RADIUS Application Example .....	399
Figure 253 WPA(2)-PSK Authentication .....	400

---

Figure 254 Security Certificate .....	403
Figure 255 Login Screen .....	404
Figure 256 Certificate General Information before Import .....	404
Figure 257 Certificate Import Wizard 1 .....	405
Figure 258 Certificate Import Wizard 2 .....	405
Figure 259 Certificate Import Wizard 3 .....	406
Figure 260 Root Certificate Store .....	406
Figure 261 Certificate General Information after Import .....	407
Figure 262 ZyXEL Device Trusted CA Screen .....	408
Figure 263 CA Certificate Example .....	409
Figure 264 Personal Certificate Import Wizard 1 .....	409
Figure 265 Personal Certificate Import Wizard 2 .....	410
Figure 266 Personal Certificate Import Wizard 3 .....	410
Figure 267 Personal Certificate Import Wizard 4 .....	411
Figure 268 Personal Certificate Import Wizard 5 .....	411
Figure 269 Personal Certificate Import Wizard 6 .....	411
Figure 270 Access the ZyXEL Device Via HTTPS .....	412
Figure 271 SSL Client Authentication .....	412
Figure 272 ZyXEL Device Secure Login Screen .....	412



# List of Tables

Table 1 NBG410W3G Front Panel Lights .....	39
Table 2 NBG412W3G Front Panel Lights .....	40
Table 3 Title Bar: Web Configurator Icons .....	47
Table 4 Web Configurator HOME Screen .....	47
Table 5 Screens Summary .....	52
Table 6 HOME > Show Statistics .....	55
Table 7 HOME > Show Statistics > Line Chart .....	56
Table 8 HOME > DHCP Table .....	57
Table 9 ISP Parameters: Ethernet Encapsulation .....	60
Table 10 ISP Parameters: PPPoE Encapsulation .....	61
Table 11 ISP Parameters: PPTP Encapsulation .....	63
Table 12 NETWORK > LAN .....	105
Table 13 NETWORK > LAN > Static DHCP .....	107
Table 14 NETWORK > LAN > IP Alias .....	109
Table 15 NETWORK > LAN > Port Roles .....	110
Table 16 NETWORK > WAN General .....	114
Table 17 Private IP Address Ranges .....	115
Table 18 NETWORK > WAN > WAN 1 (Ethernet Encapsulation) .....	118
Table 19 NETWORK > WAN > WAN 1 (PPPoE Encapsulation) .....	121
Table 20 NETWORK > WAN > WAN 1 (PPTP Encapsulation) .....	124
Table 21 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies .....	127
Table 22 NETWORK > WAN > 3G (WAN 2) .....	129
Table 23 NETWORK > WAN > Traffic Redirect .....	133
Table 24 NETWORK > DMZ .....	136
Table 25 NETWORK > DMZ > Static DHCP .....	138
Table 26 NETWORK > DMZ > IP Alias .....	140
Table 27 NETWORK > DMZ > Port Roles .....	143
Table 28 Types of Encryption for Each Type of Authentication .....	150
Table 29 WIRELESS > Wi-Fi > Wireless Card .....	152
Table 30 WIRELESS > Wi-Fi > Configuring SSID .....	154
Table 31 Security Modes .....	155
Table 32 WIRELESS > Wi-Fi > Security .....	155
Table 33 WIRELESS > Wi-Fi > Security: None .....	156
Table 34 WIRELESS > Wi-Fi > Security: WEP .....	157
Table 35 WIRELESS > Wi-Fi > Security: 802.1x Only .....	158
Table 36 WIRELESS > Wi-Fi > Security: 802.1x + Static WEP .....	159
Table 37 WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX .....	160
Table 38 WIRELESS > Wi-Fi > Security: WPA(2)-PSK .....	161

Table 39 WIRELESS > Wi-Fi > MAC Filter .....	163
Table 40 Blocking All LAN to WAN IRC Traffic Example .....	171
Table 41 Limited LAN to WAN IRC Traffic Example .....	172
Table 42 SECURITY > FIREWALL > Default Rule .....	174
Table 43 SECURITY > FIREWALL > Rule Summary .....	176
Table 44 SECURITY > FIREWALL > Rule Summary > Edit .....	179
Table 45 SECURITY > FIREWALL > Anti-Probing .....	181
Table 46 SECURITY > FIREWALL > Threshold .....	183
Table 47 SECURITY > FIREWALL > Service .....	185
Table 48 SECURITY > FIREWALL > Service > Add .....	186
Table 49 SECURITY > AUTH SERVER > Local User Database .....	193
Table 50 SECURITY > AUTH SERVER > RADIUS .....	193
Table 51 SECURITY > CERTIFICATES > My Certificates .....	198
Table 52 SECURITY > CERTIFICATES > My Certificates > Details .....	200
Table 53 SECURITY > CERTIFICATES > My Certificates > Export .....	202
Table 54 SECURITY > CERTIFICATES > My Certificates > Import .....	204
Table 55 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12 .....	204
Table 56 SECURITY > CERTIFICATES > My Certificates > Create .....	206
Table 57 SECURITY > CERTIFICATES > Trusted CAs .....	210
Table 58 SECURITY > CERTIFICATES > Trusted CAs > Details .....	212
Table 59 SECURITY > CERTIFICATES > Trusted CAs Import .....	215
Table 60 SECURITY > CERTIFICATES > Trusted Remote Hosts .....	216
Table 61 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import .....	217
Table 62 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details .....	219
Table 63 SECURITY > CERTIFICATES > Directory Servers .....	221
Table 64 SECURITY > CERTIFICATES > Directory Server > Add .....	221
Table 65 NAT Definitions .....	225
Table 66 NAT Mapping Types .....	230
Table 67 ADVANCED > NAT > NAT Overview .....	231
Table 68 ADVANCED > NAT > Address Mapping .....	233
Table 69 ADVANCED > NAT > Address Mapping > Edit .....	235
Table 70 Services and Port Numbers .....	236
Table 71 ADVANCED > NAT > Port Forwarding .....	239
Table 72 ADVANCED > NAT > Port Triggering .....	241
Table 73 ADVANCED > STATIC ROUTE > IP Static Route .....	245
Table 74 ADVANCED > STATIC ROUTE > IP Static Route > Edit .....	245
Table 75 ADVANCED > DNS > Add (Address Record) .....	251
Table 76 ADVANCED > REMOTE MGMT > WWW .....	262
Table 77 ADVANCED > REMOTE MGMT > SSH .....	269
Table 78 ADVANCED > REMOTE MGMT > Telnet .....	273
Table 79 ADVANCED > REMOTE MGMT > FTP .....	274
Table 80 SNMP Traps .....	276
Table 81 ADVANCED > REMOTE MGMT > SNMP .....	277

---

Table 82 ADVANCED > REMOTE MGMT > DNS .....	278
Table 83 ADVANCED > REMOTE MGMT > CNM .....	279
Table 84 ADVANCED > UPnP .....	282
Table 85 ADVANCED > UPnP > Ports .....	283
Table 86 ADVANCED > Custom APP .....	292
Table 87 ADVANCED > ALG .....	297
Table 88 LOGS > View Log .....	302
Table 89 Log Description Example .....	302
Table 90 LOGS > Log Settings .....	306
Table 91 LOGS > Reports .....	308
Table 92 LOGS > Reports: Web Site Hits Report .....	309
Table 93 LOGS > Reports: Host IP Address .....	310
Table 94 LOGS > Reports: Protocol/ Port .....	311
Table 95 Report Specifications .....	312
Table 96 System Maintenance Logs .....	312
Table 97 System Error Logs .....	313
Table 98 Access Control Logs .....	314
Table 99 TCP Reset Logs .....	314
Table 100 Packet Filter Logs .....	315
Table 101 ICMP Logs .....	315
Table 102 Remote Management Logs .....	315
Table 103 CDR Logs .....	316
Table 104 PPP Logs .....	316
Table 105 UPnP Logs .....	316
Table 106 Attack Logs .....	317
Table 107 3G Logs .....	318
Table 108 PKI Logs .....	319
Table 109 ACL Setting Notes .....	321
Table 110 ICMP Notes .....	321
Table 111 Syslog Logs .....	323
Table 112 RFC-2408 ISAKMP Payload Types .....	324
Table 113 MAINTENANCE > General Setup .....	326
Table 114 MAINTENANCE > Password .....	327
Table 115 MAINTENANCE > Time and Date .....	328
Table 116 MAINTENANCE > Firmware Upload .....	332
Table 117 Restore Configuration .....	334
Table 118 Typical 3G transmission speeds .....	344
Table 119 Hardware Specifications .....	345
Table 120 Firmware Specifications .....	346
Table 121 Feature Specifications .....	347
Table 122 IP Address Network Number and Host ID Example .....	378
Table 123 Subnet Masks .....	379
Table 124 Maximum Host Numbers .....	379

## List of Tables

---

Table 125 Alternative Subnet Mask Notation .....	379
Table 126 Subnet 1 .....	381
Table 127 Subnet 2 .....	382
Table 128 Subnet 3 .....	382
Table 129 Subnet 4 .....	382
Table 130 Eight Subnets .....	382
Table 131 24-bit Network Number Subnet Planning .....	383
Table 132 16-bit Network Number Subnet Planning .....	383
Table 133 Commonly Used Services .....	385
Table 134 IEEE 802.11g .....	393
Table 135 Wireless Security Levels .....	394
Table 136 Comparison of EAP Authentication Types .....	397
Table 137 Wireless Security Relational Matrix .....	400



---

# PART I

# Introduction

---

Getting to Know Your ZyXEL Device (35)

Introducing the Web Configurator (43)

Wizard Setup (59)

Tutorials (65)



# Getting to Know Your ZyXEL Device

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

## 1.1 Overview

The ZyXEL Device is a high-security 3G router with wireless capability.

Access the Internet with the 3G connection from any location with 3G coverage, with the option of using a wired WAN connection at the same time.

Enhance network security by adding a De-Militarized Zone (DMZ) to your network. This separates devices that are publicly accessible (and less secure) from your LAN.

Set up a local network with the four LAN ports and set up a wireless network with IEEE 802.11b or IEEE 802.11g compatible wireless devices. The ZyXEL Device provides the option to easily move devices from your LAN or wireless network to the DMZ.

The ZyXEL Device also provides NAT, port forwarding, DHCP server and many other powerful features.

The NBG410W3G and NBG412W3G offer similar features. However, the NBG410W3G also supports an internal 3G interface.

See [Chapter 22 on page 345](#) for a complete list of features for both devices.

## 1.2 Applications for the ZyXEL Device

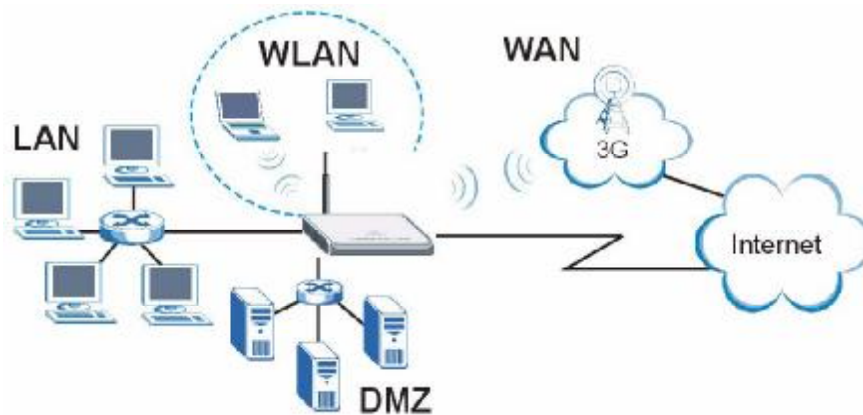
Here are some examples of what you can do with your ZyXEL Device.

### 1.2.1 3G WAN Application

With an activated, correctly inserted 3G SIM card you can use the ZyXEL Device to wirelessly access the Internet via a 3G base station. See [Section 6.9 on page 126](#) for more information about 3G.

With both the primary WAN (physical WAN port) and 3G connections enabled, you can set one of the WAN connections as a backup.

**Figure 1** 3G WAN Application



### 1.2.2 Secure Broadband Internet Access via Cable or DSL Modem

For Internet access, connect the WAN Ethernet port to your existing Internet access gateway (company network, or your cable or DSL modem for example). Connect computers or servers to the LAN or DMZ ports for shared Internet access.

The ZyXEL Device guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

**Figure 2** Secure Internet Access via Cable or DSL Modem



## 1.3 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.

## 1.4 Configuring Your ZyXEL Device's Security Features

Your ZyXEL Device comes with a variety of security features. This section summarizes these features and provides links to sections in the User's Guide to configure security settings on your ZyXEL Device. Follow the suggestions below to improve security on your ZyXEL Device and network.

### 1.4.1 Control Access to Your Device

Ensure only people with permission can access your ZyXEL Device.

- Control physical access by locating devices in secure areas, such as locked rooms. Most ZyXEL Devices have a reset button. If an unauthorized person has access to the reset button, they can then reset the device's password to its default password, log in and reconfigure its settings.
- Change any default passwords on the ZyXEL Device, such as the password used for accessing the ZyXEL Device's web configurator (if it has a web configurator). Use a password with a combination of letters and numbers and change your password regularly. Write down the password and put it in a safe place.
- Avoid setting a long timeout period before the ZyXEL Device's web configurator automatically times out. A short timeout reduces the risk of unauthorized person accessing the web configurator while it is left idle.

See [Chapter 20 on page 325](#) for instructions on changing your password and setting the timeout period.

- Configure remote management to control who can manage your ZyXEL Device. See [Section 15.1 on page 259](#) for more information. If you enable remote management, ensure you have enabled remote management only on the IP addresses, services or interfaces you intended and that other remote management settings are disabled.

### 1.4.2 Wireless Security

Wireless devices are especially vulnerable to attack. If your ZyXEL Device has a wireless function, take the following measures to improve wireless security.

- Enable wireless security on your ZyXEL Device. Choose the most secure encryption method that all devices on your network support. If you have a RADIUS server, enable IEEE 802.1x or WPA(2) user identification on your network so users must log in. This method is more common in business environments.
- Hide your wireless network name (SSID). The SSID can be regularly broadcast and unauthorized users may use this information to access your network.
- Enable the MAC filter to allow only trusted users to access your wireless network or deny unwanted users access based on their MAC address.

See [Section 8.2 on page 148](#) for directions on these wireless security measures.

### 1.4.3 Firewall

See [Section 9.1 on page 167](#) for more information on the following security measures

- Ensure the firewall is turned on. Traffic initiated from your WAN is blocked by default.

- Set the firewall to block ICMP requests.
- Enable do not respond to requests for unauthorized services.
- If you have a backup gateway (for example, backup Internet access) on your network, disable the Bypass Triangle Routes feature and enable IP Alias to put your backup gateway on a different subnet.
- Avoid raising the maximum number of NAT sessions per host unnecessarily as it increases the possibility of unauthorized connections, such as connections caused by a computer virus.

#### 1.4.4 NAT

- Enable NAT (Network Address Translation) to make devices on your network “invisible” to those outside your network (unless you configure port-forwarding rules for them).
- Applications such as games or file-sharing can be configured so they are visible from other networks by using port-forwarding. Ensure only applications you want are configured to port-forward.

See [Section 12.1 on page 225](#) for instructions on these measures.

#### 1.4.5 UPnP

- Disable UPnP (Universal Plug and Play) unless you specifically want applications (for example, games or file-sharing applications) on your network to pass through your firewall unchecked.

See [Section 16.1 on page 281](#) for instructions on this measure.

### 1.5 Maintaining Your ZyXEL Device

Do the following things regularly to keep your ZyXEL Device running.

- Check the ZyXEL website ([www.zyxel.com.tw](http://www.zyxel.com.tw)) regularly for new firmware for your ZyXEL Device.



---

Ensure you download the correct firmware for your model.

---

- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.





## 1.5.1 Front Panel Lights

**Figure 3** Front Panel





The following tables describe the lights. Table 1 describes the light features in NBG410W3G, and Table 2 describes the light features in NBG412W3G.





**Table 1** NBG410W3G Front Panel Lights

LED	ICONS	COLOR	STATUS	DESCRIPTION
<b>POWER</b>			Off	The ZyXEL Device is turned off.
		Green	On	The ZyXEL Device is ready and running.
			Flashing	The ZyXEL Device is restarting.
		Red	On	The power to the ZyXEL Device is too low.
<b>LAN/DMZ 10/100</b>			Off	The LAN/DMZ is not connected.
		Green	On	The ZyXEL Device has a successful 10Mbps Ethernet connection.
			Flashing	The 10M LAN is sending or receiving packets.
		Orange	On	The ZyXEL Device has a successful 100Mbps Ethernet connection.
	Flashing	The 100M LAN is sending or receiving packets.		
<b>WAN</b>			Off	The WAN connection is not ready, or has failed.
		Green	On	The ZyXEL Device has a successful 10Mbps WAN connection.
			Flashing	The 10M WAN is sending or receiving packets.
		Orange	On	The ZyXEL Device has a successful 100Mbps WAN connection.
	Flashing	The 100M WAN is sending or receiving packets.		
<b>Wi-Fi</b>		Green	Off	The wireless connection through the built-in Wi-Fi card is not ready, or has failed.
			On	The wireless LAN through the built-in wireless LAN card is ready.
			Flashing	The wireless LAN through the built-in wireless LAN card is sending or receiving packets.

**Table 1** NBG410W3G Front Panel Lights (continued)



LED	ICONS	COLOR	STATUS	DESCRIPTION
<b>3G OPERATION</b>		Green	On	The ZyXEL Device has a successful 3G connection.
			Flashing	The ZyXEL Device has detected an available 3G network, but has not yet connected to it.
		Blue	On	The ZyXEL Device has a successful 3.5G connection
			Flashing	The ZyXEL Device has detected an available 3.5G network, but has not yet connected to it.
		Orange	On	The ZyXEL Device has a successful 2G or 2.5G connection
			Flashing	The ZyXEL Device has detected an available 2G or 2.5G network, but has not yet connected to it.
	Off	One (or more) of the following has occurred. <ul style="list-style-type: none"> <li>The 3G function is not activated.</li> <li>The ZyXEL Device is not registered with a 3G network.</li> </ul>		
<b>3G SIGNAL STRENGTH</b>		Green	On	The 3G signal is strong.
		Yellow		The 3G signal is moderate.
		Red		The 3G signal is weak.
			Off	If the <b>3G OPERATION</b> LED is not off, no 3G signal is detected.

**Table 2** NBG412W3G Front Panel Lights

LED	ICONS	COLOR	STATUS	DESCRIPTION
<b>POWER</b>			Off	The ZyXEL Device is turned off.
		Green	On	The ZyXEL Device is ready and running.
			Flashing	The ZyXEL Device is restarting.
		Red	On	The power to the ZyXEL Device is too low.
<b>LAN/DMZ 10/100</b>			Off	The LAN/DMZ is not connected.
		Green	On	The ZyXEL Device has a successful 10Mbps Ethernet connection.
			Flashing	The 10M LAN is sending or receiving packets.
		Orange	On	The ZyXEL Device has a successful 100Mbps Ethernet connection.
Flashing	The 100M LAN is sending or receiving packets.			
<b>WAN</b>			Off	The WAN connection is not ready, or has failed.
		Green	On	The ZyXEL Device has a successful 10Mbps WAN connection.
			Flashing	The 10M WAN is sending or receiving packets.
		Orange	On	The ZyXEL Device has a successful 100Mbps WAN connection.
Flashing	The 100M WAN is sending or receiving packets.			
<b>Wi-Fi</b>		Green	Off	The wireless connection through the built-in Wi-Fi card is not ready, or has failed.
			On	The wireless LAN through the built-in wireless LAN card is ready.
			Flashing	The wireless LAN through the built-in wireless LAN card is sending or receiving packets.



**Table 2** NBG412W3G Front Panel Lights (continued)

LED	ICONS	COLOR	STATUS	DESCRIPTION
<b>3G MODE</b>		Green	On	The 3G function is activated.
			Off	The 3G function is not activated.
<b>3G LINK</b>		Green	On	The ZyXEL Device has a successful 3G connection.
			Off	There is no 3G connection .



# Introducing the Web Configurator

This chapter describes how to access the ZyXEL Device web configurator and provides an overview of its screens.

## 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 [Appendix A on page 353](#) if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

## 2.2 Accessing the ZyXEL Device Web Configurator

- 1 Make sure your ZyXEL Device hardware is properly connected and prepare your computer/computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

**Figure 4** Login Screen



- 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

**Figure 5** Change Password Screen



- 6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device.



---

If you do not replace the default certificate here or in the **CERTIFICATES** screen, this screen displays every time you access the web configurator.

---

**Figure 6** Replace Certificate Screen



- 7 You should now see the **HOME** screen (see [Figure 9 on page 47](#)).



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 reload the factory-default configuration file or use the **RESET** button on the back of the ZyXEL Device. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to 1234, also.

### 2.3.1 Procedure To Use The Reset Button

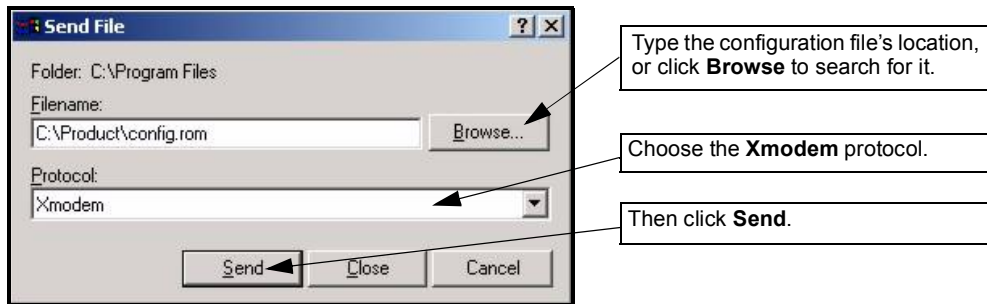
Make sure the **POWER** LED is on (not blinking) before you begin this procedure.

- 1 Press the **RESET** button for ten seconds, and then release it. If the **POWER** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts. Otherwise, go to step 2.
- 2 Turn the ZyXEL Device off.
- 3 While pressing the **RESET** button, turn the ZyXEL Device on.
- 4 Continue to hold the **RESET** button. The **POWER** LED will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the ZyXEL Device is now restarting.
- 5 Release the **RESET** button and wait for the ZyXEL Device to finish restarting.

### 2.3.2 Uploading a Configuration File Via Console Port

- 1 Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.
- 2 Turn off the ZyXEL Device, begin a terminal emulation software session and turn on the ZyXEL Device again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.
- 3 Enter "y" at the prompt below to go into debug mode.
- 4 Enter "atlc" after "Enter Debug Mode" message.
- 5 Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

**Figure 7** Example Xmodem Upload

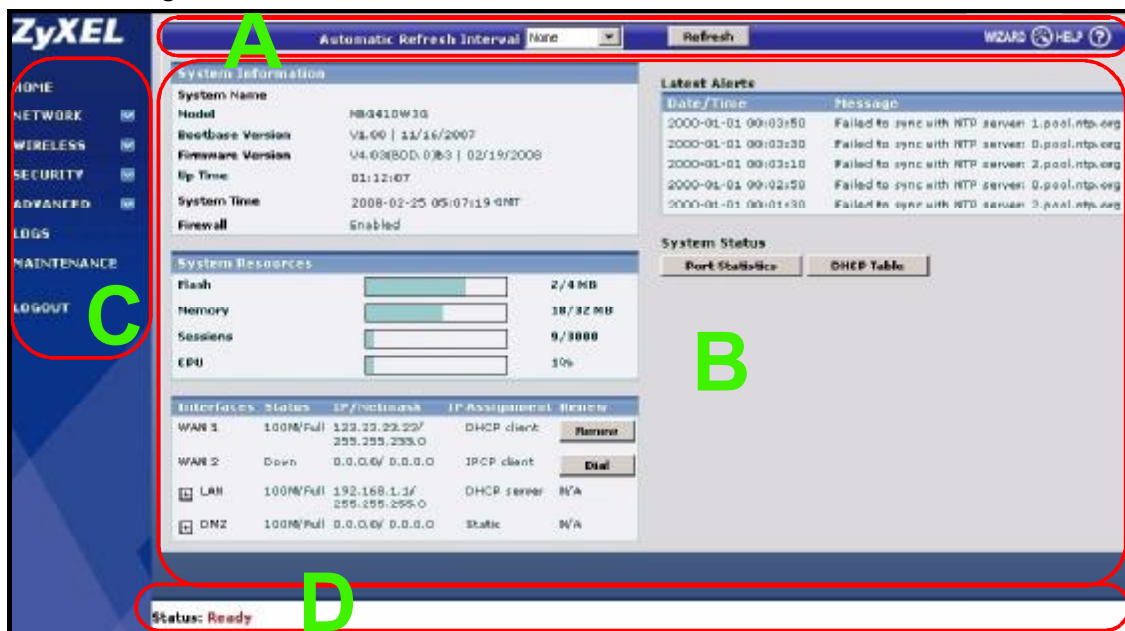


6 After successful firmware upload, enter "atgo" to restart the router.

## 2.4 Navigating the ZyXEL Device Web Configurator

The following summarizes how to navigate the web configurator from the **HOME** screen.

**Figure 8** HOME Screen



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



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

### 2.4.1 Title Bar

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

The icons provide the following functions.

**Table 3** Title Bar: Web Configurator Icons

ICON	DESCRIPTION
	<b>Wizard</b> Click this icon to open one of the web configurator wizards. See <a href="#">Chapter 3 on page 59</a> for more information.
	<b>Help</b> Click this icon to open the help page for the current screen.

## 2.4.2 Main Window

The main window shows the screen you select in the navigation panel. It is discussed in more detail in the rest of this document.

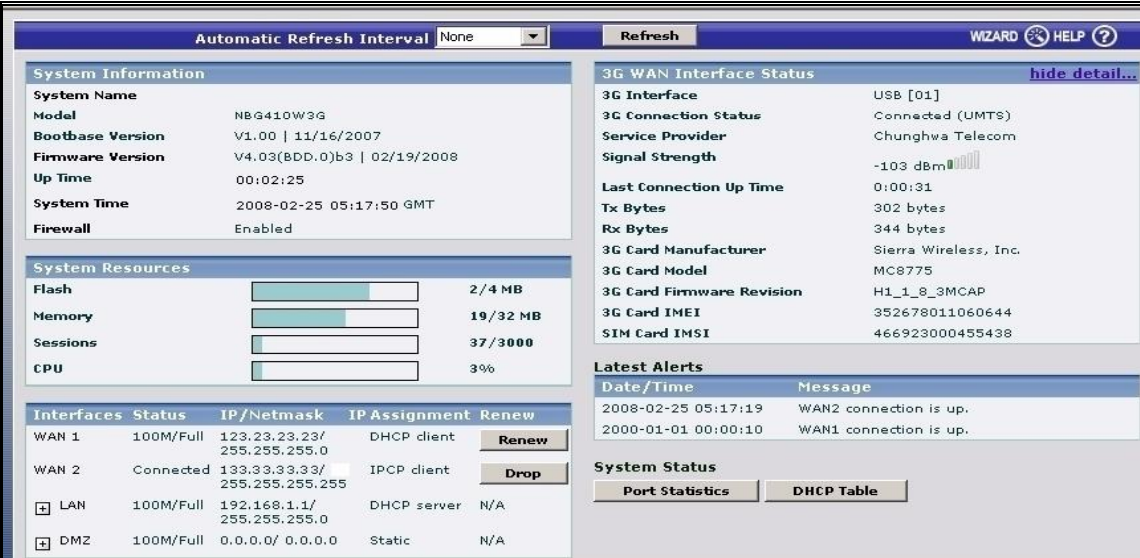
Right after you log in, the **HOME** screen is displayed.

## 2.4.3 HOME Screen

This screen displays general status information about the ZyXEL Device.

WAN 2 refers to the 3G feature on the supported ZyXEL Device.

**Figure 9** Web Configurator HOME Screen



The following table describes the labels in this screen.

**Table 4** Web Configurator HOME Screen

LABEL	DESCRIPTION
Automatic Refresh Interval	Select a number of seconds or <b>None</b> from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the status screen statistics immediately.

**Table 4** Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
System Information	
System Name	This is the <b>System Name</b> you enter in the <b>MAINTENANCE &gt; General</b> screen. It is for identification purposes. Click the field label to go to the screen where you can specify a name for this ZyXEL Device.
Model	This is the model name of your ZyXEL Device.
Bootbase Version	This is the bootbase version and the date created.
Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. Click the field label to go to the screen where you can upload a new firmware file.
Up Time	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you turn it on, when you restart it ( <b>MAINTENANCE &gt; Restart</b> ), or when you reset it (see <a href="#">Section 2.3 on page 45</a> ).
System Time	This field displays your ZyXEL Device's present date (in yyyy-mm-dd format) and time (in hh:mm:ss format) along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyXEL Device to use it. Click the field label to go to the screen where you can modify the ZyXEL Device's date and time settings.
Firewall	This displays whether or not the ZyXEL Device's firewall is activated. Click the field label to go to the screen where you can turn the firewall on or off.
System Resources	
Flash	The first number shows how many megabytes of the flash the ZyXEL Device is using.
Memory	The first number shows how many megabytes 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 and the firewall. The second number shows the ZyXEL Device's total heap memory (in megabytes). 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.
Sessions	The first number shows how many sessions are currently open on the ZyXEL Device. This includes all sessions that are currently traversing the ZyXEL Device, terminating at the ZyXEL Device or Initiated from the ZyXEL Device The second number is the maximum number of sessions that can be open at one time. The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached.
CPU	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
Interfaces	This is the port type. Click "+" to expand or "-" to collapse the IP alias drop-down lists. Hold your cursor over an interface's label to display the interface's MAC address. Click an interface's label to go to the screen where you can configure settings for that interface.



**Table 4** Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
Status	<p>For the LAN and DMZ ports, this displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.</p> <p>For the WAN 1 port, it displays the port speed and duplex setting if you're using Ethernet encapsulation or the remote node name for a PPP connection and <b>Down</b> (line is down or not connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) or <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation.</p> <p>For the WAN 2 interface, it displays <b>Connected</b> when the 3G connection is up, <b>Connecting</b> when the 3G card is trying to connect to a network but has not received a response from the base station, <b>Ready to Connect</b> when the 3G connection is idle, <b>Initializing</b> when the ZyXEL Device is configuring the 3G card with AT commands, <b>Disconnecting</b> when the ZyXEL Device is dropping the 3G connection or <b>Down</b> when the 3G connection is down.</p>
IP/Netmask	This shows the port's IP address and subnet mask.
IP Assignment	<p>For the WAN, if the ZyXEL Device gets its IP address automatically from an ISP, this displays <b>DHCP client</b> when you're using Ethernet encapsulation and <b>IPCP Client</b> when you're using PPPoE or PPTP encapsulation. <b>Static</b> displays if the WAN port is using a manually entered static (fixed) IP address.</p> <p>For the LAN or DMZ, <b>DHCP server</b> displays when the ZyXEL Device is set to automatically give IP address information to the computers connected to the LAN. <b>DHCP relay</b> displays when the ZyXEL Device is set to forward IP address assignment requests to another DHCP server. <b>Static</b> displays if the LAN port is using a manually entered static (fixed) IP address. In this case, you must have another DHCP server on your LAN, or else the computers must be manually configured.</p>
Renew	If you are using Ethernet encapsulation and the WAN port is configured to get the IP address automatically from the ISP, click <b>Renew</b> to release the WAN port's dynamically assigned IP address and get the IP address afresh. Click <b>Dial</b> to dial up the PPTP, PPPoE or 3G WAN connection. Click <b>Drop</b> to disconnect the PPTP, PPPoE or 3G WAN connection.
3G WAN Interface Status	The fields below display when a 3G card is inserted and WAN 2 is enabled.
show detail.../hide detail...	Click <b>show detail...</b> to see more information about the 3G connection and 3G card. Click <b>hide detail...</b> to display less information about the 3G connection and 3G card.
3G Connection Status	<p>This displays <b>Down</b> when the 3G connection is down or not activated.</p> <p>This displays <b>Initializing</b> when the ZyXEL Device is configuring the 3G card with AT commands.</p> <p>This displays <b>Ready to Connect</b> when the 3G connection is idle before the ZyXEL Device triggers a call.</p> <p>This displays <b>Connecting</b> when the 3G card is trying to connect to a network but has not received a response from the base station.</p> <p>This displays <b>Connected</b> when the 3G connection is up.</p> <p>This displays <b>Disconnecting</b> when the ZyXEL Device is dropping the 3G connection.</p> <p>This field also displays the type of the network to which the ZyXEL Device is connected. The network type varies depending on the 3G card you inserted and could be <b>UMTS</b>, <b>HSDPA</b>, <b>GPRS</b> or <b>EDGE</b> when you insert a GSM 3G card, or <b>1xRTT</b>, <b>EVDO Rev.0</b> or <b>EVDO Rev.A</b> when you insert a CDMA 3G card.</p>
Service Provider	This displays the name of your network service provider or <b>Limited Service</b> when the signal strength is too low or the ISP is limiting your access.

**Table 4** Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
Roaming Network	This field is available only when you insert a 3G card that supports the roaming feature. This displays whether the card is able to connect to other ISPs' base stations.
Dormant State	This field is available only when you insert a 3G card that supports the dormant state. This displays whether the card is in dormant state. When there is no data transmitting, a card does not send a radio signal and is in dormant state to reduce bandwidth usage.
Signal Strength	This displays the signal strength of the wireless network in dBm. The status bar shows the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your ZyXEL Device and the service provider's base station. You can see a signal strength indication even when the ZyXEL Device does not have a 3G connection (because the signal is still there even when the ZyXEL Device is not using it).
Last Connection Up Time	This displays how long the 3G connection has been up.
Tx Bytes	This displays the total number of data frames transmitted.
Rx Bytes	This displays the total number of data frames received.
3G Card Manufacturer	This displays the manufacturer of your 3G card.
3G Card Model	This displays the model name of your 3G card.
3G Card Firmware Revision	This displays the version of the firmware currently used in the 3G card.
3G Card IMEI	This field is available only when you insert a GSM (Global System for Mobile Communications) or UMTS (Universal Mobile Telecommunications System) 3G card. This displays the International Mobile Equipment Identity (IMEI) which is the serial number of the GSM or UMTS 3G wireless card. The IMEI is a unique 15-digit number used to identify a mobile device.
SIM Card IMSI	This field is available only when you insert a GSM or UMTS 3G card. This displays the International Mobile Subscriber Identity (IMSI) stored in the SIM (Subscriber Identity Module) card. The SIM card is installed in a mobile device and used for authenticating a customer to the carrier network. The IMSI is a unique 15-digit number used to identify a user on a network.
3G Card ESN	This field is available only when you insert a CDMA (Code Division Multiple Access) 3G card. This shows the ESN (Electronic Serial Number) of the inserted CDMA 3G card. The ESN is the serial number of a CDMA 3G card and is similar to the IMEI on a GSM or UMTS 3G card.
Enter PIN code again	If the PIN code you specified in the <b>3G (WAN 2)</b> screen is not the right one for the card you inserted, this field displays allowing you to enter the correct PIN code. Enter the PIN code (four to eight digits) for the inserted 3G card.
Apply	Click <b>Apply</b> to save the correct PIN code and replace the one you specified in the <b>3G (WAN 2)</b> screen.
PUK Code	If you enter the PIN code incorrectly three times, the SIM card will be blocked by your ISP and you cannot use the account to access the Internet. You should get the PUK (Personal Unblocking Key) code (four to eight digits) from your ISP. Enter the PUK code to enable the SIM card. If an incorrect PUK code is entered 10 times, the SIM card will be disabled permanently. You then need to contact your ISP for a new SIM card.

**Table 4** Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
New PIN Code	Configure a PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code or enter the previous PIN code.
Confirm New PIN Code	Enter the PIN code again for confirmation.
Apply	Click <b>Apply</b> to save your changes in this section.
Reset budget counters, resume budget control	This field displays if you have enabled budget control but insert a 3G card with a different user account from the one for which you configured budget control. Select this option to have the ZyXEL Device do budget calculation starting from 0 but use the previous settings.
Resume budget control	This field displays if you have enabled budget control but insert a 3G card with a different user account from the one for which you configured budget control. Select this option to have the ZyXEL Device keep the existing statistics and continue counting.
Disable budget control	This field displays if you have enabled budget control but insert a 3G card with a different user account from the one for which you configured budget control. Select this option to disable budget control. If you want to enable and configure new budget control settings for the new user account, go to the <b>3G (WAN 2)</b> screen. The ZyXEL Device keeps the existing statistics if you do not change the budget control settings. You could reinsert the original card and enable budget control to have the ZyXEL Device continue counting the budget control statistics.
Apply	Click <b>Apply</b> to save your changes in this section.
Enter modem unlock code	This field only displays when you insert a 3G card and the internal modem on the 3G card is blocked. Enter a key to enable the internal modem on your 3G card. By default, the key is the last four digits of your phone number used to dial up the 3G connection. Otherwise, you need to get the key from your service provider.
Apply	Click <b>Apply</b> to save your changes in this section.
Remaining Time Budget	This field is available only when you enable budget control in the <b>3G (WAN 2)</b> screen. This shows the amount of time (in hours and minutes) the 3G connection can still be used before the ZyXEL Device takes the actions you specified in the <b>3G (WAN 2)</b> screen.
Remaining Data Budget	This field is available only when you enable budget control in the <b>Network &gt; WAN &gt; 3G (WAN 2)</b> screen. This shows how much data (in bytes) can still be transmitted through the 3G connection before the ZyXEL Device takes the actions you specified in the <b>3G (WAN 2)</b> screen.  <b>Note:</b> The budget counters will not be reset when you restore the factory defaults. The budget counters are saved to the flash every hour or when the 3G connection is dropped. If you restart the ZyXEL Device within one hour, any change in the counters will not be saved.
Reset time and data budget counters	This button is available only when you enable budget control in the <b>3G (WAN 2)</b> screen. Click this button to reset the time and data budgets. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart.

**Table 4** Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
Latest Alerts	This table displays the five most recent alerts recorded by the ZyXEL Device. You can see more information in the <b>View Log</b> screen, such as the source and destination IP addresses and port numbers of the incoming packets.
Date/Time	This is the date and time the alert was recorded.
Message	This is the reason for the alert.
System Status	
Port Statistics	Click <b>Port Statistics</b> to see router performance statistics such as the number of packets sent and number of packets received for each port.
DHCP Table	Click <b>DHCP Table</b> to show current DHCP client information.
Bandwidth	Click <b>Bandwidth</b> to view the ZyXEL Device's bandwidth usage and allotments.

## 2.4.4 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure ZyXEL Device features.

The following table describes the sub-menus.

**Table 5** Screens Summary

LINK	TAB	FUNCTION
HOME		This screen shows the ZyXEL Device's general device and network status information. Use this screen to access the wizards, statistics and DHCP table.
NETWORK		
LAN	LAN	Use this screen to configure LAN DHCP and TCP/IP settings.
	Static DHCP	Use this screen to assign fixed IP addresses on the LAN.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Port Roles	Use this screen to change the LAN/DMZ port roles.
WAN	General	This screen allows you to configure operation mode, route priority and connection test.
	WAN1	Use this screen to configure the WAN1 connection for Internet access.
	3G (WAN2)	Use this screen to configure the WAN2 connection for Internet access.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.
DMZ	DMZ	Use this screen to configure your DMZ connection.
	Static DHCP	Use this screen to assign fixed IP addresses on the DMZ.
	IP Alias	Use this screen to partition your DMZ interface into subnets.
	Port Roles	Use this screen to change the LAN/DMZ port roles on the ZyXEL Device.
WIRELESS		
3G (WAN2)	3G (WAN2)	Use this screen to configure the WAN2 connection for Internet access.

**Table 5** Screens Summary (continued)

LINK	TAB	FUNCTION
Wi-Fi	Wireless Card	Use this screen to configure the wireless LAN settings.
	Security	Use this screen to configure the Wi-Fi security settings.
	MAC Filter	Use this screen to change MAC filter settings on the ZyXEL Device
SECURITY		
FIREWALL	Default Rule	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti-Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
	Service	Use this screen to configure custom services.
CERTIFICATES	My Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CAs	Use this screen to view and manage the list of the trusted CAs.
	Trusted Remote Hosts	Use this screen to view and manage the certificates belonging to the trusted remote hosts.
	Directory Servers	Use this screen to view and manage the list of the directory servers.
AUTH SERVER	Local User Database	Use this screen to configure the local user account(s) on the ZyXEL Device.
	RADIUS	Configure this screen to use an external server to authenticate wireless users.
ADVANCED		
NAT	NAT Overview	Use this screen to enable NAT.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Port Forwarding	Use this screen to configure servers behind the ZyXEL Device.
	Port Triggering	Use this screen to change your ZyXEL Device's port triggering settings.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.
DNS	System	Use this screen to configure the address and name server records.
	Cache	Use this screen to configure the DNS resolution cache.
	DHCP	Use this screen to configure LAN/DMZ DNS information.
	DDNS	Use this screen to set up dynamic DNS.

**Table 5** Screens Summary (continued)

LINK	TAB	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.
	SSH	Use this screen to configure through which interface(s) and from which IP address(es) users can use Secure Shell 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.
	CNM	Use this screen to configure and allow your ZyXEL Device to be managed by the Vantage CNM server.
UPnP	UPnP	Use this screen to enable UPnP on the ZyXEL Device.
	Ports	Use this screen to view the NAT port mapping rules that UPnP creates on the ZyXEL Device.
Custom APP	Custom APP	Use this screen to specify port numbers for the ZyXEL Device to monitor for FTP, HTTP, SMTP, POP3, H323, and SIP traffic.
ALG	ALG	Use this screen to allow certain applications to pass through the ZyXEL Device.
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.
	Reports	Use this screen to have the ZyXEL Device record and display the network usage reports.
MAINTENANCE	General	This screen contains administrative.
	Password	Use this screen to change your password.
	Time and Date	Use this screen to change your ZyXEL Device's time and date.
	F/W Upload	Use this screen to upload firmware to your ZyXEL Device
	Backup & Restore	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.
LOGOUT		Click this label to exit the web configurator.

### 2.4.5 Port Statistics

Click **Port Statistics** in the **HOME** screen. Read-only information here includes port status and packet specific statistics. The **Automatic Refresh Interval** field is configurable.

Figure 10 HOME &gt; Show Statistics

Port	Status	TxPkts	RxPkts	Tx B/s	Rx B/s	Up Time
WAN 1	100M/Full	415	694	0	0	0:16:15
WAN 2	Idle	19	12	0	0	0:00:00
LAN	100M/Full	1616	1611	90	0	0:16:17
DMZ	100M/Full	18	0	0	0	0:16:15
WLAN Card	Down	14	0	0	0	00:00:00

System Up Time : 0:16:29

Automatic Refresh Interval:  Refresh

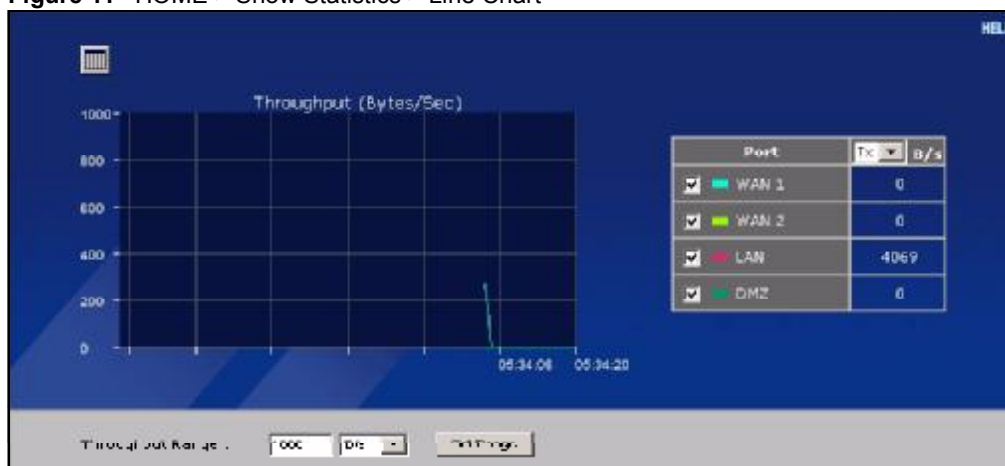
The following table describes the labels in this screen.

Table 6 HOME &gt; Show Statistics

LABEL	DESCRIPTION
	Click the icon to display the chart of throughput statistics.
Port	These are the ZyXEL Device's interfaces.
Status	For the WAN interface(s), this displays the port speed and duplex setting if you're using Ethernet encapsulation or the remote node name for a PPP connection and <b>Down</b> (line is down or not connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) or <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation. For the LAN or DMZ ports, this displays the port speed and duplex setting. For the Wi-Fi card, this displays the transmission rate when Wi-Fi is enabled or <b>Down</b> when Wi-Fi is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyXEL Device has been on.
Automatic Refresh Interval	Select a number of seconds or <b>None</b> from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen's statistics immediately.

## 2.4.6 Show Statistics: Line Chart

Click the icon in the **Show Statistics** screen. This screen shows you a line chart of each port's throughput statistics.

**Figure 11** HOME > Show Statistics > Line Chart

The following table describes the labels in this screen.

**Table 7** HOME > Show Statistics > Line Chart

LABEL	DESCRIPTION
	Click the icon to go back to the <b>Show Statistics</b> screen.
Port	Select the check box(es) to display the throughput statistics of the corresponding interface(s).
B/s	Specify the direction of the traffic for which you want to show throughput statistics in this table. Select <b>Tx</b> to display transmitted traffic throughput statistics and the amount of traffic (in bytes). Select <b>Rx</b> to display received traffic throughput statistics and the amount of traffic (in bytes).
Throughput Range	Set the range of the throughput (in <b>B/s</b> , <b>KB/s</b> or <b>MB/s</b> ) to display. Click <b>Set Range</b> to save this setting back to the ZyXEL Device.

### 2.4.7 DHCP Table Screen

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

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



Figure 12 HOME &gt; DHCP Table

HOME - DHCP TABLE

Interface

#	IP Address	Host Name	MAC Address	Reserve <input type="checkbox"/>
1	192.168.1.33	tw11	00:00:e8:7c:14:80	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 8 HOME &gt; DHCP Table

LABEL	DESCRIPTION
Interface	Select <b>LAN</b> or <b>DMZ</b> to show the current DHCP client information for the specified interface.
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table. After you click <b>Apply</b> , the MAC address and IP address also display in the corresponding <b>LAN</b> or <b>DMZ Static DHCP</b> screen (where you can edit them).
Refresh	Click <b>Refresh</b> to reload the DHCP table.



# 3

## Wizard Setup

This chapter provides information on the **Wizard Setup** screens in the web configurator.

### 3.1 Wizard Setup Overview

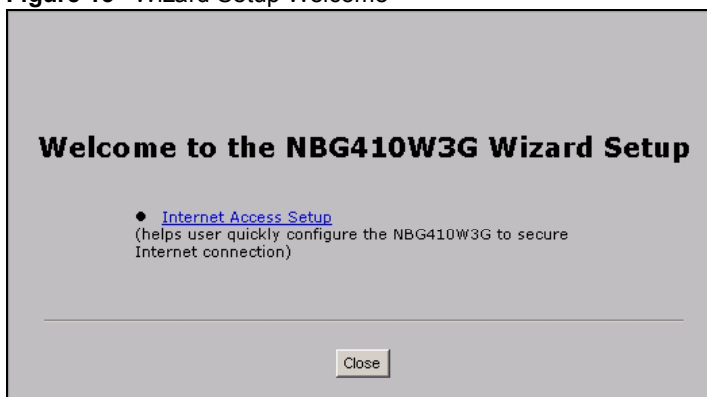
The web configurator's setup wizards help you configure Internet connection settings.

In the **HOME** screen, click the wizard icon  to open the **Wizard Setup Welcome** screen. The following summarizes the wizards you can select:

- **Internet Access Setup**

Click this link to open a wizard to set up an Internet connection for **WAN 1** (the WAN port) on the ZyXEL Device.

**Figure 13** Wizard Setup Welcome



### 3.2 Internet Access

The Internet access wizard screen has three variations depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

#### 3.2.1 ISP Parameters

The ZyXEL Device offers three choices of encapsulation. They are **Ethernet**, **PPTP** or **PPPoE**.

The wizard screen varies according to the type of encapsulation that you select in the **Encapsulation** field.

### 3.2.1.1 Ethernet

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyXEL Device** firewall rule for those packets. Contact your ISP to find the correct port number.

Choose **Ethernet** when the WAN port is used as a regular Ethernet port.

**Figure 14** ISP Parameters: Ethernet Encapsulation

**WIZARD - Internet Access**

**ISP Parameters for Internet Access**

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

**WAN IP Address Assignment**

IP Address Assignment:

My WAN IP Address:

My WAN IP Subnet Mask:

Gateway IP Address:

First DNS Server:

Second DNS Server:

The following table describes the labels in this screen.

**Table 9** ISP Parameters: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet. Otherwise, choose <b>PPPoE</b> or <b>PPTP</b> for a dial-up connection.
WAN IP Address Assignment	
IP Address Assignment	Select <b>Dynamic</b> if your ISP did not assign you a fixed IP address. This is the default selection. Select <b>Static</b> if the ISP assigned a fixed IP address. The fields below are available only when you select <b>Static</b> .
My WAN IP Address	Enter your WAN IP address in this field.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.

**Table 9** ISP Parameters: Ethernet Encapsulation

LABEL	DESCRIPTION
Gateway IP Address	Enter the gateway IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as <b>0.0.0.0</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Back	Click <b>Back</b> to return to the previous wizard screen.
Finish	Click <b>Finish</b> to save your changes and go to the next screen.

### 3.2.1.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

**Figure 15** ISP Parameters: PPPoE Encapsulation

The screenshot shows a wizard window titled "WIZARD - Internet Access". Inside, there are two main sections: "ISP Parameters for Internet Access" and "WAN IP Address Assignment".

**ISP Parameters for Internet Access:**

- Encapsulation: A dropdown menu set to "PPP over Ethernet".
- Service Name: A text input field with "(Optional)" to its right.
- User Name: A text input field.
- Password: A text input field with asterisks.
- Retype to Confirm: A text input field with asterisks.
- Nailed-Up
- Idle Timeout: A text input field with "100" and "(Seconds)" to its right.

**WAN IP Address Assignment:**

- IP Address Assignment: A dropdown menu set to "Dynamic".

At the bottom right, there are "Back" and "Finish" buttons.

The following table describes the labels in this screen.

**Table 10** ISP Parameters: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose an encapsulation method from the pull-down list box. <b>PPP over Ethernet</b> forms a dial-up connection.
Service Name	Type the name of your service provider.

**Table 10** ISP Parameters: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is <b>100</b> seconds.
WAN IP Address Assignment	
IP Address Assignment	Select <b>Dynamic</b> if your ISP did not assign you a fixed IP address. This is the default selection. Select <b>Static</b> if the ISP assigned a fixed IP address. The fields below are available only when you select <b>Static</b> .
My WAN IP Address	Enter your WAN IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as <b>0.0.0.0</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Back	Click <b>Back</b> to return to the previous wizard screen.
Finish	Click <b>Finish</b> to save your changes and go to the next screen.

### 3.2.1.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.



The ZyXEL Device supports one PPTP server connection at any given time.

**Figure 16** ISP Parameters: PPTP Encapsulation

**WIZARD - Internet Access**

**ISP Parameters for Internet Access**

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation: PPTP

User Name: [ ]

Password: [ ]

Retype to Confirm: [ ]

Nailed-Up

Idle Timeout: 100 (Seconds)

**PPTP Configuration**

My IP Address: 0 . 0 . 0 . 0

My IP Subnet Mask: 0 . 0 . 0 . 0

Server IP Address: 0 . 0 . 0 . 0

Connection ID/Name: [ ]

**WAN IP Address Assignment**

IP Address Assignment: Dynamic

Back Finish

The following table describes the labels in this screen.

**Table 11** ISP Parameters: PPTP Encapsulation

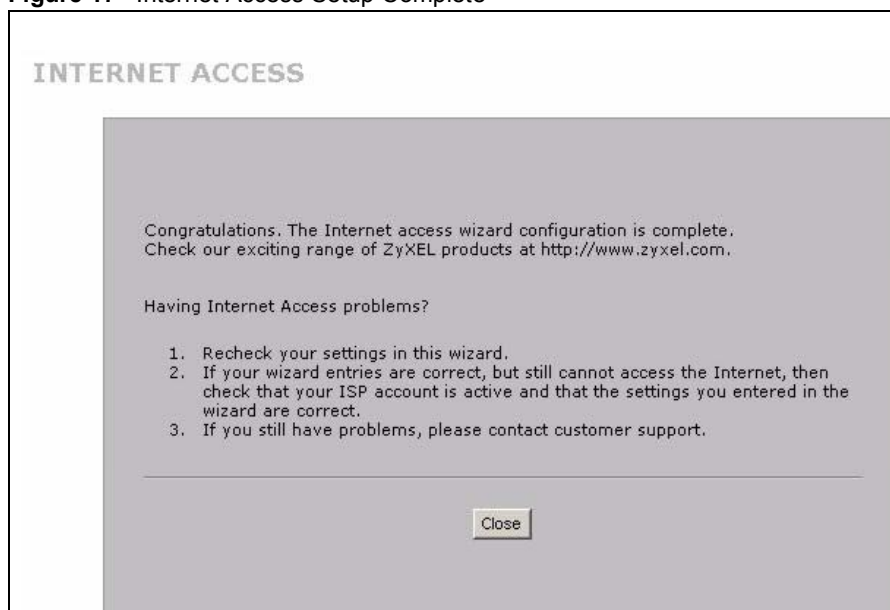
LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select <b>PPTP</b> from the drop-down list box. To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.

**Table 11** ISP Parameters: PPTP Encapsulation

LABEL	DESCRIPTION
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your xDSL modem.
WAN IP Address Assignment	
IP Address Assignment	Select <b>Dynamic</b> If your ISP did not assign you a fixed IP address. This is the default selection. Select <b>Static</b> If the ISP assigned a fixed IP address. The fields below are available only when you select <b>Static</b> .
My WAN IP Address	Enter your WAN IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as <b>0.0.0.0</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Back	Click <b>Back</b> to return to the previous wizard screen.
Finish	Click <b>Finish</b> to save your changes and go to the next screen.

### 3.2.2 Internet Access Wizard Setup Complete

The congratulations screen displays. Click **Close** to complete the Internet access setup.

**Figure 17** Internet Access Setup Complete



# 4

## Tutorials

This section describes how to do the following.

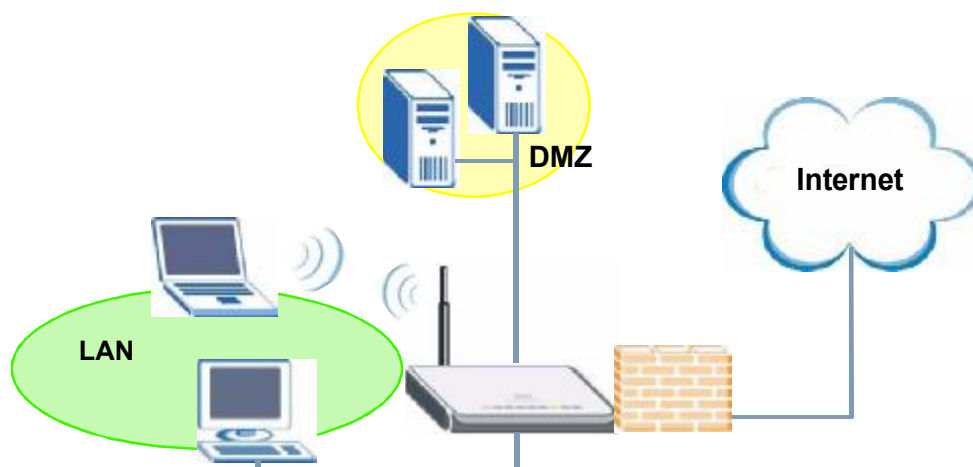
- 1 Set up a DMZ (De-Militarized Zone).
- 2 Use an H.323 VoIP phone on your LAN.
- 3 Use NAT (Network Address Translation) with multiple public IP addresses.
- 4 Allow multiple game players to connect to the same server.

### 4.1 DMZ Overview

The DMZ is a separate network for devices that provide services to users on the Internet. Devices such as a web or e-mail server are more prone to security threats as they are more visible from the Internet and more frequently accessed than devices on your LAN. By placing such devices on a DMZ, you can better restrict access to the devices on your LAN.

The diagram shows servers on the DMZ which are open to public access but protected by the ZyXEL Device's firewall. Devices which require greater security are located on the LAN.

**Figure 18** DMZ Overview



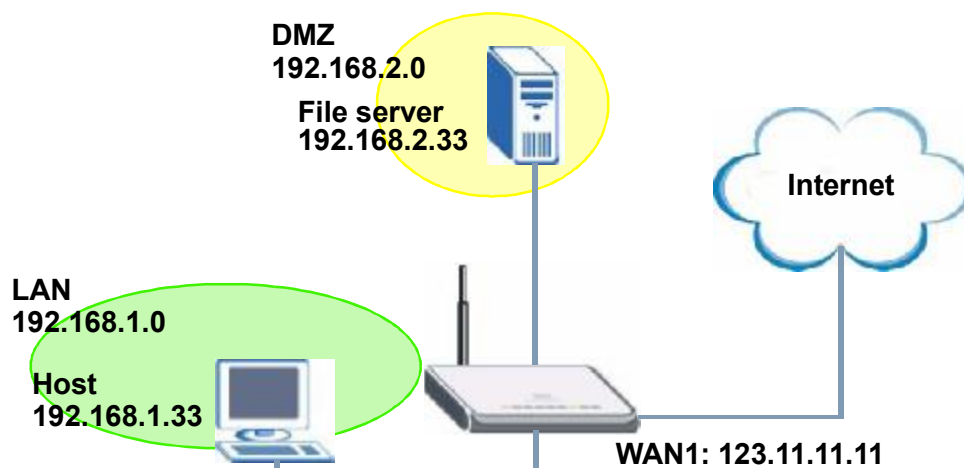
In this situation a file server is located in the DMZ. The file server is available for public access from the Internet and also from computers located on the LAN.

You can use either public or private IP addresses for your DMZ, however the DMZ must be on a different subnet or network from the LAN.

## 4.2 DMZ Setup Example

In this example the DMZ uses private IP addresses and the default subnet mask of 255.255.255.0. (See [Appendix C on page 377](#) for information on subnetting.) You can also use a static public IP address for your file server.

**Figure 19** DMZ Tutorial: DMZ Setup



### 4.2.1 Basic Setup

Follow these steps to set up your DMZ with a private or a public IP address.

#### 4.2.1.1 Private IP Address

- 1 Click **NETWORK > DMZ** to open the **DMZ** screen. In the **DMZ TCP/IP** field type your DMZ IP address in the **IP address** field. In the **IP Subnet Mask** field type the same subnet mask as that used on the LAN.
- 2 Select **Server** from the drop-down list in the **DHCP** field to have the ZyXEL Device dynamically assign IP addresses to devices on the DMZ. In the **IP Pool Starting Address** field type the first available IP address for the DMZ subnetwork. In this example 192.168.2.33 is used. Skip to [Section 4.2.1.3 on page 67](#).

#### 4.2.1.2 Public IP Address

Either configure a static IP address on the server directly using the server's operating system, or follow these steps to set up static DHCP on the ZyXEL Device.

- 1 Click **NETWORK > DMZ > Static DHCP** to open the **Static DHCP** screen.
- 2 Type the MAC address of the file server in the **MAC Address** field and a valid IP address on your DMZ in the **IP Address** field. In this example the MAC address is 00:A0:C5:00:00:02 and the IP address is 192.168.2.33.
- 3 Click **Apply**. That completes setup of static DHCP on the ZyXEL Device.

Figure 20 DMZ Tutorial: NETWORK &gt; DMZ &gt; Static DHCP

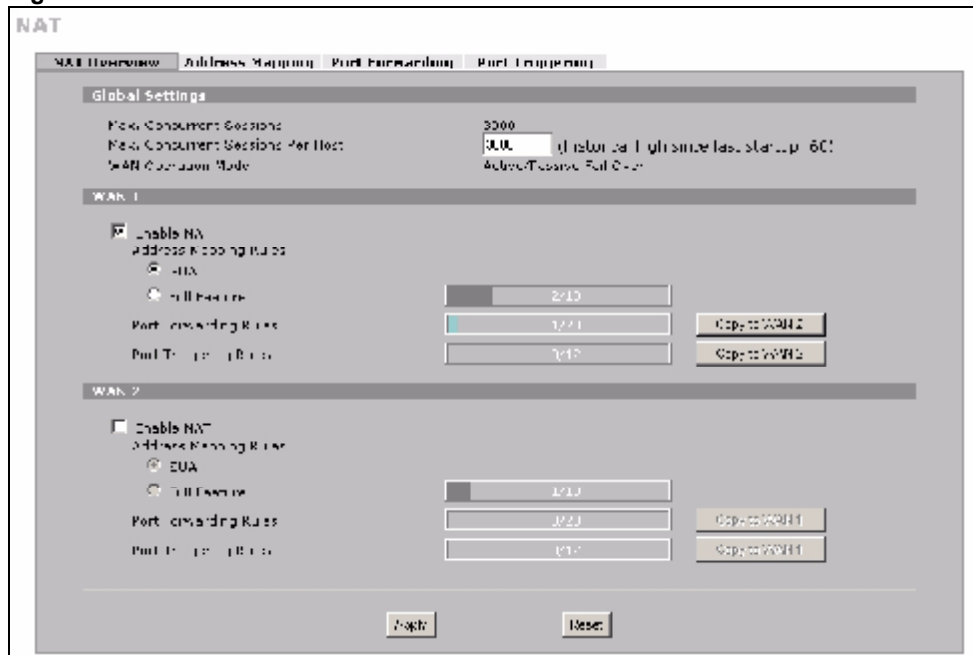
#	MAC Address	IP Address
1	0C:4C:2D:C0:C2	192.168.2.20
2		0.0.0.0
3		0.0.0.0
4		0.0.0.0
5		0.0.0.0
6		0.0.0.0
7		0.0.0.0
8		0.0.0.0

#### 4.2.1.3 Public and Private IP Addresses

- 1 In **Windows Networking (NetBIOS over TCP/IP)** select **Allow between DMZ and LAN**. In this example, both the file server on the DMZ and a computer on the LAN use a Windows OS. Enable NetBIOS to allow LAN computers to use Windows programs such as Windows Explorer to access the server on the DMZ.
- 2 Click **Apply**.

Figure 21 DMZ Tutorial: NETWORK &gt; DMZ

- 3 Ensure NAT (Network Address Translation) is enabled on your WAN to allow the ZyXEL Device to manage the IP addresses of traffic it routes between networks. Click **ADVANCED > NAT**. For your WAN connection select . In this example NAT is enabled in the **Enable NAT** field on WAN1 and **SUA** is selected. For more information on this screen see [Chapter 12 on page 225](#).

**Figure 22** DMZ Tutorial: ADVANCED > NAT Overview

This completes basic setup of your DMZ.

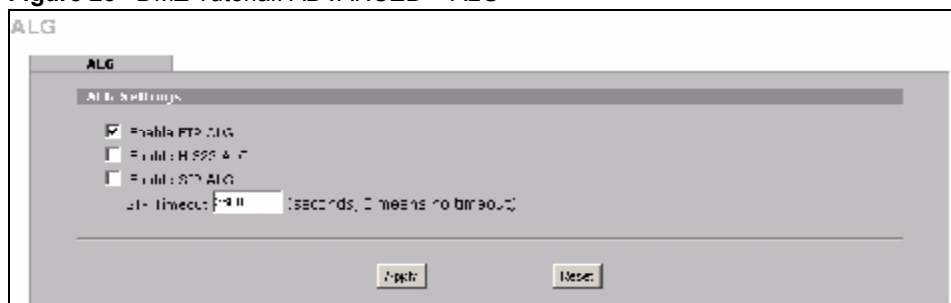
## 4.2.2 Advanced Setup

In this scenario the file server runs an FTP (File Transfer Protocol) download service. Since FTP is not compatible with NAT, you can use the ALG (Application Layer Gateway) to manage FTP. (See [Chapter 18 on page 293](#) for more information.)

To allow FTP sessions to be initiated by users on the WAN, port-forwarding is also required (see [Section 12.5 on page 235](#) for more information) and for port-forwarding the file server needs a static IP address.

### ALG Setup

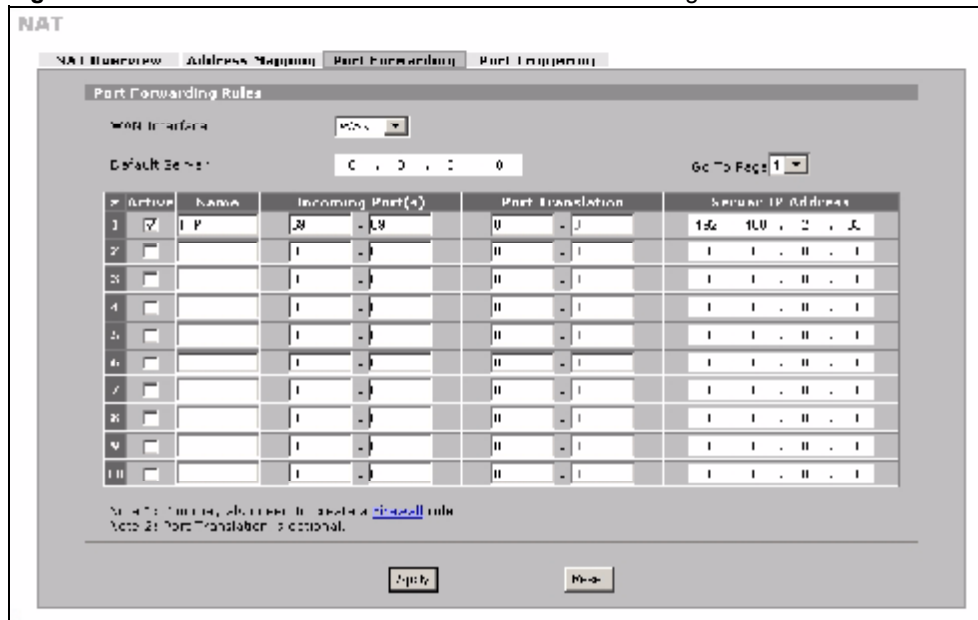
To turn on the ZyXEL Device's FTP ALG, click **ADVANCED > ALG**. Select **Enable FTP ALG** and click **Apply**.

**Figure 23** DMZ Tutorial: ADVANCED > ALG

### Port Forwarding Setup

- 1 To configure port forwarding, first configure a static IP on the file server if you haven't already. See [Section 4.2.1.2 on page 66](#).
- 2 Click **ADVANCED > NAT > Port Forwarding** to open the **Port Forwarding** screen.
- 3 In the **WAN Interface** field select the correct WAN for your network. This example uses **WAN1**.
- 4 In the rule row you are configuring select **Active**.
- 5 In the **Name** field type a descriptive name for the port forwarding rule. This example uses **FTP**.
- 6 In the **Incoming Port(s)** field type the port number used by the FTP application. This example uses **69**.
- 7 In the **Server IP Address** field type the IP address of your file server. This example uses **192.168.1.33**.
- 8 Click **Apply**.

**Figure 24** DMZ Tutorial: ADVANCED > NAT > Port Forwarding



This completes setup of NAT-incompatible services on the server in your DMZ. Now users can access the file server on your DMZ from the Internet.

## 4.3 Firewall Rule Setup

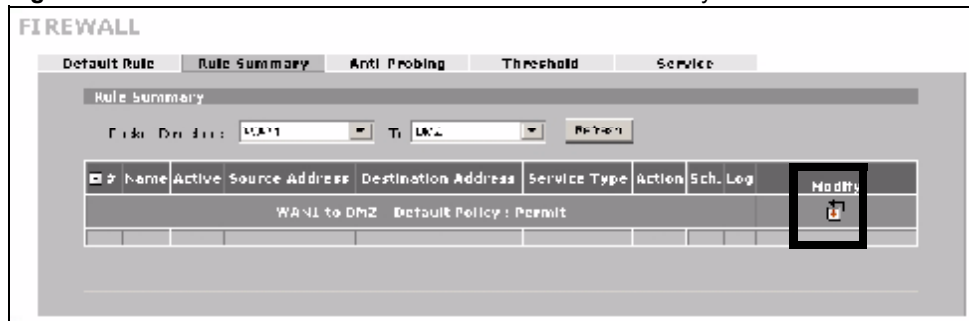
Your ZyXEL Device's firewall default settings provide network security by allowing traffic from the WAN to your DMZ, and blocking traffic from the DMZ to the LAN. However, you can further enhance network security by defining firewall rules specifically for traffic from the WAN to the DMZ.

You need to define two rules - one to drop all traffic from the WAN to the DMZ, the other to permit HTTP and FTP traffic from the WAN to the DMZ. This ensures that only HTTP and FTP traffic from the WAN to the DMZ is permitted and all other traffic is blocked.

If you have not already done so, define a static IP address for the file server (see step 1 on page 69 for instructions).

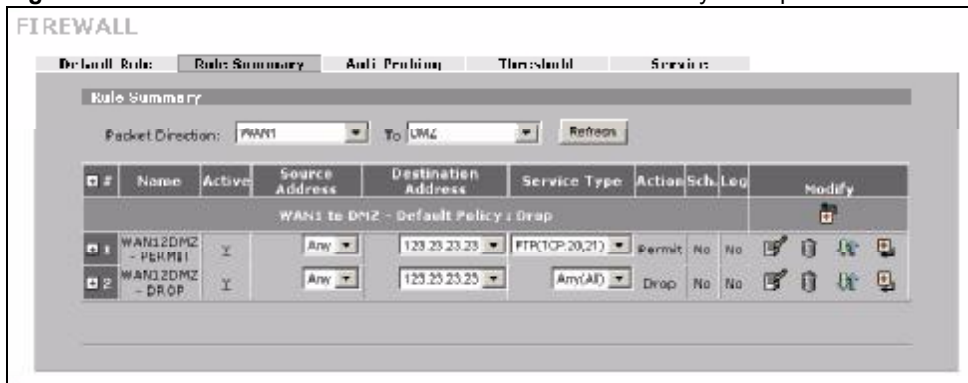
- 1 Click **SECURITY > Firewall > Rule Summary** to display the **Rule Summary** screen. Use this screen to configure firewall rules on traffic between the file server and the WAN. In this example, traffic from WAN1 to the the file server is restricted to HTTP and FTP traffic.
- 2 The **Rule Summary** screen appears. Select **WAN1** and **DMZ** from the drop-down list in the **Packet Direction** field and click **Refresh**. Click the **Modify** (🔧) icon to add a new rule.

**Figure 25** DMZ Tutorial: SECURITY > Firewall > Rule Summary



- 3 The **Firewall - Edit** screen appears. Type the name of the firewall rule in the **Rule Name** field. In this example WAN12DMZ - DENY is used.
- 4 In the **Edit Source Address** section select **Any Address** in the drop-down box in the **Address Type** field to define the source address of traffic from the Internet as any IP address.
- 5 In the **Edit Destination Address** section select **Single Address** in the drop-down box in the **Address Type** field. Type the destination address of traffic in the **Start IP Address** field. In this case the WAN1 IP address is used - 123.23.23.23. If you are using a public static IP address for your web server, type the server's IP address in this field.
- 6 Click **Add** so that the IP address appears in the **Destination Address(es)** field.
- 7 In the **Edit Service** section of the **Firewall - Edit** screen select **Any** so that they appear in the **Selected Service(s)** field.
- 8 In the **Action for Matched Packets** field select **Drop** from the drop-down box.
- 9 In the **Edit Service** section select **FTP** and click the arrow icon. Then select **HTTP** and click the arrow icon again so that **FTP** and **HTTP** appear in the **Selected Service(s)** field.
- 10 Click **Apply**.

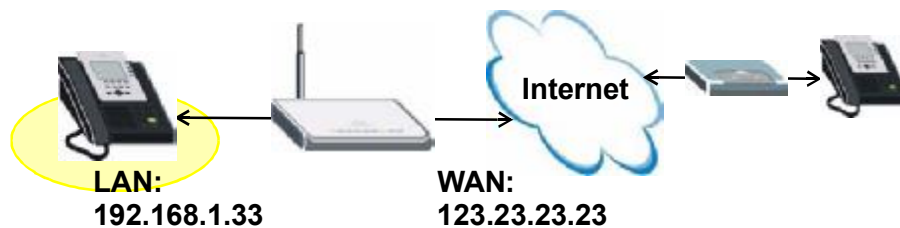


**Figure 27** DMZ Tutorial: SECURITY > Firewall > Rule Summary Example

This completes setup of a firewall rules for the file server on your DMZ.

## 4.4 Setting Up a VoIP Phone with H.323

You can use the ZyXEL Device to manage calls from your VoIP enabled phone using H.323. The following diagram shows an example of a VoIP phone configured to make calls over the Internet.

**Figure 28** Tutorial: H.323 Phone Setup

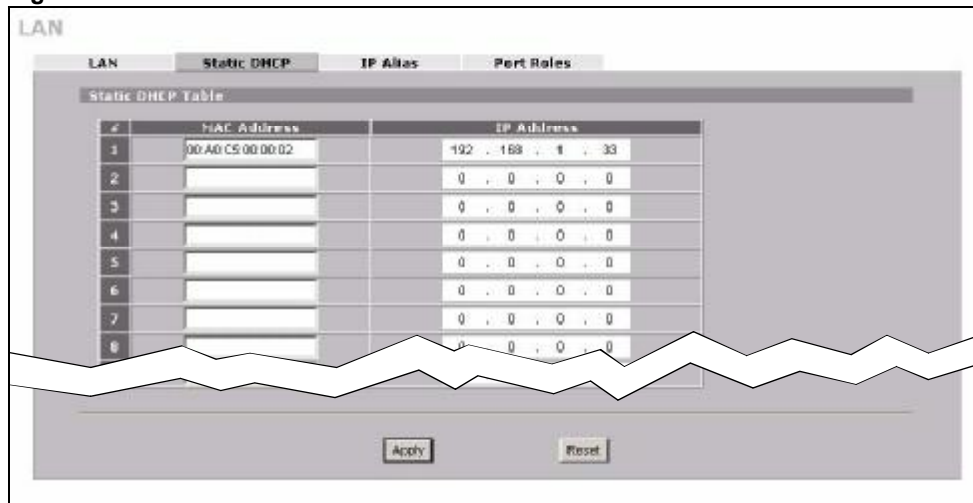
To configure your ZyXEL Device to allow VoIP phone calls using your H.323 phone, you need to set up the H.323 ALG (Application Layer Gateway) and port forwarding, which in turn requires a fixed IP address for your phone.

### IP Address Settings

Follow these steps to give your phone a fixed IP address.

- 1 Click **NETWORK > LAN > Static DHCP** to open the **Static DHCP** screen.
- 2 Type the MAC address of your device in the **MAC Address** field and a valid IP address on your LAN in the **IP Address** field. In this example the MAC address is 00:A0:C5:00:00:02 and the IP address is 192.168.1.33.
- 3 Click **Apply**.



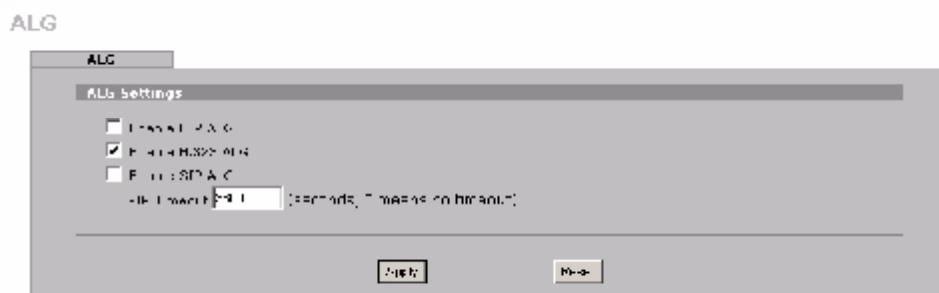
**Figure 29** H.323 Tutorial: NETWORK > LAN > Static DHCP

- 4 Click **NETWORK > LAN** to display the **LAN** screen. Ensure that **Server** is selected in the drop-down box in the **DHCP** field.

### Set up ALG

Follow these steps to set up ALG (Application Layer Gateway) to let your ZyXEL Device manage H.323 traffic. (For more information on ALG see [Chapter 18 on page 293](#).)

- 1 Click **ADVANCED > ALG** to display the **ALG** screen. Select **Enable H.323 ALG** and click **Apply**. This configures ALG (Application Layer Gateway) to manage H.323 traffic through your ZyXEL Device.
- 2 Click **Apply**.

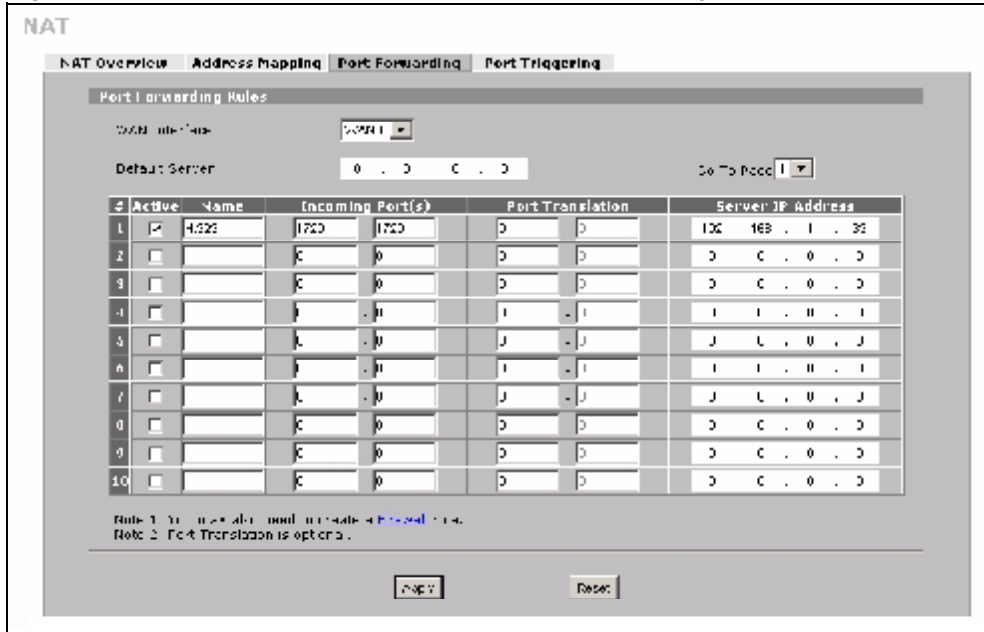
**Figure 30** H.323 Tutorial: ADVANCED > ALG

### Set up Port Forwarding

- 1 Click **ADVANCED > NAT > Port Forwarding** to display the **Port Forwarding** screen.
- 2 Select the correct WAN for your network in the **WAN Interface** field.
- 3 Select **Active** in the rule row you are configuring.
- 4 Type a descriptive name for the port forwarding rule in the **Name** field. In this example H.323 is used.
- 5 Type 1720 in the **Incoming Port(s)** field. This port number is used for the H.323 services.

- 6 Type the IP address of your VoIP phone in the **Server IP Address** field. In this example 192.168.1.33 is used.
- 7 Click **Apply**.

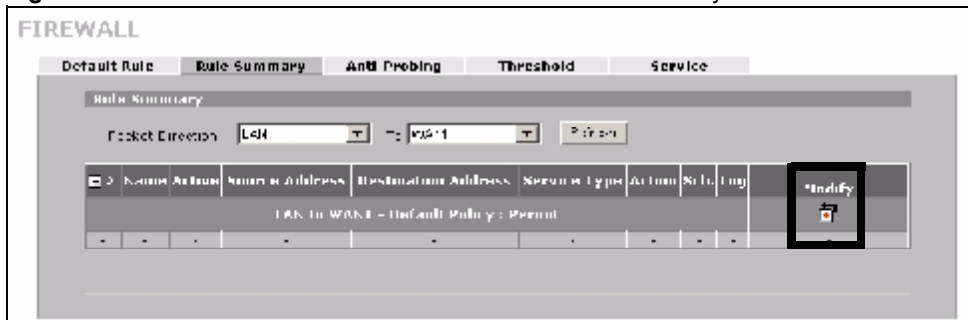
**Figure 31** H.323 Tutorial: ADVANCED > NAT > Port Forwarding



**Set up a Firewall Rule**

- 1 Click **SECURITY > Firewall > Rule Summary** to display the **Rule Summary** screen and to configure firewall rules on traffic between the VoIP phone and the WAN. In this example, traffic between the file server and WAN1 is restricted to H.323 traffic.
- 2 The **Rule Summary** screen appears. Select **DMZ** and **WAN1** from the drop-down list in the **Packet Direction** field and click **Refresh**. Click the **Modify** (🔧) icon to add a new rule.

**Figure 32** H.323 Tutorial: SECURITY > Firewall > Rule Summary



- 3 The **Firewall - Edit** screen appears. Type the name of the firewall rule in the **Rule Name** field. In this example LAN2WAN1 - H.323 is used.
- 4 In the **Edit Source Address** section select **Single Address** in the drop-down box in the **Address Type** field. Type the source address of H.323 traffic in the **Start IP Address**

field - 123.23.23.23 and click **Add** so that the IP address appears in the **Destination Address(es)** field. If you are using a H.323 server, use its IP address instead.

- 5** In the **Edit Destination Address** section select **Single Address** in the drop-down box in the **Address Type** field. Type the destination address of H.323 traffic in the Start IP Address field - 192.168.1.33 and click **Add** so that the IP address appears in the **Source Address(es)** field.
- 6** In the **Edit Service** section select **H.323** and click the arrow icon so that **H.323** appears in the **Selected Service(s)** field.
- 7** Click **Apply**.

**Figure 33** H.323 Tutorial: SECURITY > Firewall > Rule Summary

**FIREWALL - EDIT RULE**

Rule Name:

---

**Edit Source Address**

Address E-IP:       From Address List:

Address Type:

Start IP Address:      

End IP Address:      

Standard Host:      

---

**Edit Destination Address**

Address E-IP:       Destination Address List:

Address Type:

Start IP Address:      

End IP Address:      

Standard Host:      

---

**Edit Service**

Available Services (E-IP: [SERVICES](#))

FTP (TCP/21)
HTTP (TCP/80)
HTTPS (TCP/443)
IRC (TCP/6666)
MSRPC (TCP/135)
MSRPC (TCP/136)
MSRPC (TCP/137)
MSRPC (TCP/138)
MSRPC (TCP/139)
MSRPC (TCP/140)
MSRPC (TCP/141)
MSRPC (TCP/142)
MSRPC (TCP/143)
MSRPC (TCP/144)
MSRPC (TCP/145)
MSRPC (TCP/146)
MSRPC (TCP/147)
MSRPC (TCP/148)
MSRPC (TCP/149)
MSRPC (TCP/150)
MSRPC (TCP/151)
MSRPC (TCP/152)
MSRPC (TCP/153)
MSRPC (TCP/154)
MSRPC (TCP/155)
MSRPC (TCP/156)
MSRPC (TCP/157)
MSRPC (TCP/158)
MSRPC (TCP/159)
MSRPC (TCP/160)
MSRPC (TCP/161)
MSRPC (TCP/162)
MSRPC (TCP/163)
MSRPC (TCP/164)
MSRPC (TCP/165)
MSRPC (TCP/166)
MSRPC (TCP/167)
MSRPC (TCP/168)
MSRPC (TCP/169)
MSRPC (TCP/170)
MSRPC (TCP/171)
MSRPC (TCP/172)
MSRPC (TCP/173)
MSRPC (TCP/174)
MSRPC (TCP/175)
MSRPC (TCP/176)
MSRPC (TCP/177)
MSRPC (TCP/178)
MSRPC (TCP/179)
MSRPC (TCP/180)
MSRPC (TCP/181)
MSRPC (TCP/182)
MSRPC (TCP/183)
MSRPC (TCP/184)
MSRPC (TCP/185)
MSRPC (TCP/186)
MSRPC (TCP/187)
MSRPC (TCP/188)
MSRPC (TCP/189)
MSRPC (TCP/190)
MSRPC (TCP/191)
MSRPC (TCP/192)
MSRPC (TCP/193)
MSRPC (TCP/194)
MSRPC (TCP/195)
MSRPC (TCP/196)
MSRPC (TCP/197)
MSRPC (TCP/198)
MSRPC (TCP/199)
MSRPC (TCP/200)
MSRPC (TCP/201)
MSRPC (TCP/202)
MSRPC (TCP/203)
MSRPC (TCP/204)
MSRPC (TCP/205)
MSRPC (TCP/206)
MSRPC (TCP/207)
MSRPC (TCP/208)
MSRPC (TCP/209)
MSRPC (TCP/210)
MSRPC (TCP/211)
MSRPC (TCP/212)
MSRPC (TCP/213)
MSRPC (TCP/214)
MSRPC (TCP/215)
MSRPC (TCP/216)
MSRPC (TCP/217)
MSRPC (TCP/218)
MSRPC (TCP/219)
MSRPC (TCP/220)
MSRPC (TCP/221)
MSRPC (TCP/222)
MSRPC (TCP/223)
MSRPC (TCP/224)
MSRPC (TCP/225)
MSRPC (TCP/226)
MSRPC (TCP/227)
MSRPC (TCP/228)
MSRPC (TCP/229)
MSRPC (TCP/230)
MSRPC (TCP/231)
MSRPC (TCP/232)
MSRPC (TCP/233)
MSRPC (TCP/234)
MSRPC (TCP/235)
MSRPC (TCP/236)
MSRPC (TCP/237)
MSRPC (TCP/238)
MSRPC (TCP/239)
MSRPC (TCP/240)
MSRPC (TCP/241)
MSRPC (TCP/242)
MSRPC (TCP/243)
MSRPC (TCP/244)
MSRPC (TCP/245)
MSRPC (TCP/246)
MSRPC (TCP/247)
MSRPC (TCP/248)
MSRPC (TCP/249)
MSRPC (TCP/250)
MSRPC (TCP/251)
MSRPC (TCP/252)
MSRPC (TCP/253)
MSRPC (TCP/254)
MSRPC (TCP/255)

Selected Services:

H323 (TCP/173)
----------------

---

**Edit Schedule**

Days to Apply:

Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Apply (24-hour format):

All day

Start:  :  (Hour) :  (Minute)      End:  :  (Hour) :  (Minute)

---

**Actions When Matched**

Log Packet Information When Matched

Send Alert Message When Matched (Default: 1)

Action for Matched Packets:

- 8 Repeat the firewall rule setup procedure to add a similar firewall rule for H.323 traffic from the WAN to the LAN, using the same WAN IP address and LAN IP address settings.
- 9 In the **Rule Summary** screen select **Any** and **Any** from the drop-down list in the **Packet Direction** fields and click **Refresh** to check your firewall rule settings.

**Figure 34** H.323 Tutorial: SECURITY > Firewall > Rule Summary

That completes setup of your H.323 VoIP phone.

## 4.5 Using NAT with Multiple Public IP Addresses

This section shows you examples of how to set up your ZyXEL Device if you have more than one fixed (static) IP address from your ISP.

### 4.5.1 Example Parameters and Scenario

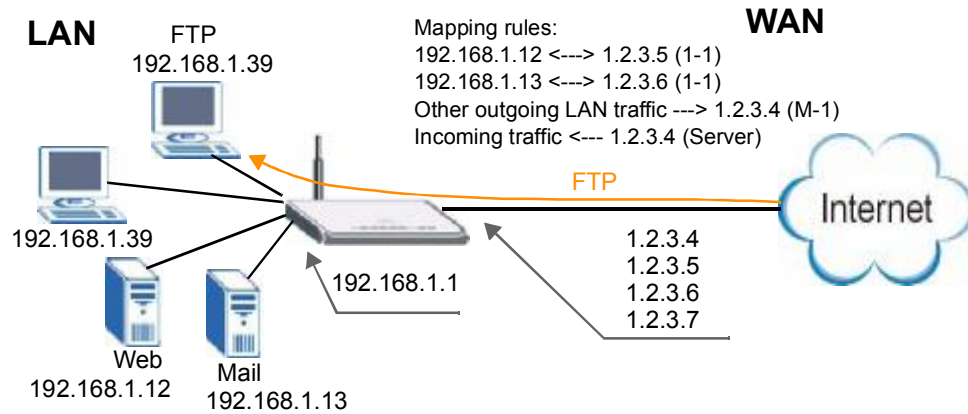
The following table shows the public IP addresses from your ISP and your ZyXEL Device's LAN IP address.

<b>Public IP Addresses</b>	1.2.3.4 to 1.2.3.7
<b>ZyXEL Device's LAN IP Address</b>	192.168.1.1

The following figure shows the network you want to set up in this example.

- Assign the first public address (1.2.3.4) to the ZyXEL Device's WAN 1 port.
- Map the second and third public IP addresses (1.2.3.5 and 1.2.3.6) to the web and mail servers (192.168.1.12 and 192.168.1.13) respectively for traffic in both directions.
- Map the first public address (1.2.3.4) to outgoing traffic from other local computers.
- Map the first public address (1.2.3.4) to incoming traffic from WAN 1.
- Forward FTP traffic using port 21 from WAN 1 to a specific local computer (192.168.1.39).
- The last public IP address (1.2.3.7) is not mapped to any device and is reserved for future use.

**Figure 35** Tutorial Example: Using NAT with Static Public IP Addresses



To set up this network, we are going to:

- 1 Configure the WAN 1 connection to use the first public IP address (1.2.3.4).
- 2 Configure NAT address mapping for other public IP addresses (1.2.3.5 and 1.2.3.6).
- 3 Configure NAT port forwarding to forward FTP traffic from WAN 1 to a specific computer on your local network.

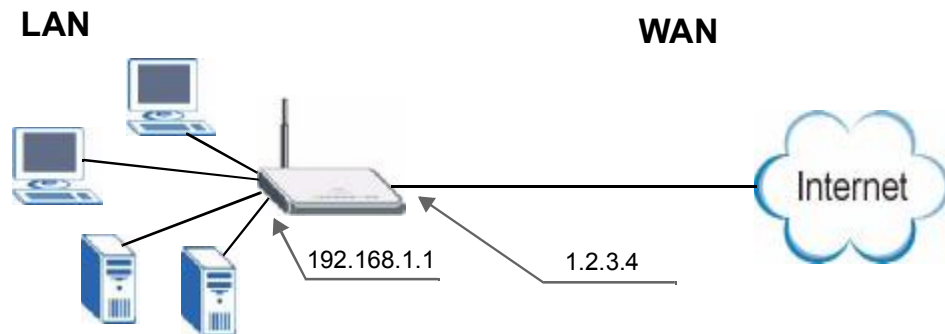
### 4.5.2 Configuring the WAN Connection with a Static IP Address

The following table shows the information your ISP gave you for Internet connection.

<b>Encapsulation</b>	PPPoE
<b>Public IP Addresses</b>	1.2.3.4 1.2.3.5 1.2.3.6 1.2.3.7
<b>Gateway IP Address</b>	1.2.3.89
<b>Subnet Mask</b>	255.255.255.0
<b>User Name</b>	exampleuser
<b>Password</b>	abcd1234
<b>DNS Server</b>	1.2.1.1 1.2.1.2

Follow the steps below to configure your ZyXEL Device for Internet access using PPPoE in this example.

**Figure 36** Tutorial Example: WAN Connection with a Static Public IP Address



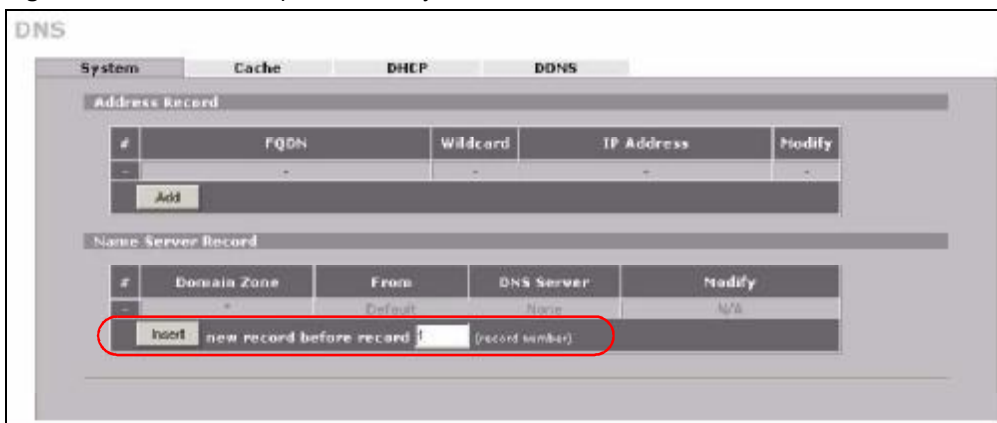
- 1 Click **NETWORK > WAN > WAN 1**.
- 2 Select **PPPoE (PPP over Ethernet)** from the **Encapsulation** drop-down list box.
- 3 In the **ISP Parameters for Internet Access** section, enter the information (such as the user name and password) provided by your ISP. If your ISP didn't give you the service name, leave the field blank.
- 4 In the **WAN IP Address Assignment** section, select **Use Fixed IP Address** and enter the first fixed public IP address (1.2.3.4 in this example).
- 5 Click **Apply**.

**Figure 37** Tutorial Example: WAN 1 Screen

- 6 Click **ADVANCED > DNS**.

- 7 The **System** screen displays. Click the **Insert** button to configure the IP address of the DNS server the ZyXEL Device can query to resolve domain names.

**Figure 38** Tutorial Example: DNS > System



- 8 Select **Public DNS Server** and enter the first DNS server’s IP address given by your ISP. Click **Apply**.

**Figure 39** Tutorial Example: DNS > System Edit-1



- 9 Enter the rule number (2) where you want to put the second record and click the **Insert** button to configure the second DNS server’s IP address as follows. Click **Apply**.



To resolve a domain name, the ZyXEL Device checks it against the name server record entries in the order that they appear in this list.



**Figure 40** Tutorial Example: DNS > System Edit-2

**DNS - EDIT NAME SERVER RECORD**

Name Server Record

Domain Zone\*

\* optional. Leave this field blank if all domain zones are served by the specified DNS server(s).

DNS Server

DNS Server(s) from ISP

First DNS Server	Second DNS Server	Third DNS Server
N/A	N/A	N/A

Public DNS Server

Private DNS Server

Apply Cancel

**10** The DNS > System screen should look as shown.

**Figure 41** Tutorial Example: DNS > System: Done

**DNS**

System Cache DHCP DDNS

Address Record

#	FQDN	wildcard	IP Address	Modify
-	*	*	*	*

Add

Name Server Record

#	Domain Zone	From	DNS Server	Modify
1	*	User-Defined	1.2.1.1	△ ▾ ⌨ 🗑
2	*	User-Defined	1.2.1.2	△ ▾ ⌨ 🗑
-	*	Default	None	N/A

Insert new record before record  (record number)

**11** Go to the **Home** screen to check your WAN connection status. Make sure the status is not down.

Figure 42 Tutorial Example: Status

The screenshot displays the status page of a ZyXEL device. It is divided into several sections:

- System Information:** Model: NBG410W3G, Bootbase Version: V1.00 | 11/24/2007, Firmware Version: V4.03(BDD-0)63 | 02/19/2008, Up Time: 00:02:25, System Time: 2008-02-25 05:17:00 GMT, Firewall: Enabled.
- System Resources:** Flash: 2/4 MB, Memory: 19/32 MB, Sessions: 37/3000, CPU: 3%.
- 3G WAN Interface Status:** 3G Interface: USB [01], 3G Connection Status: Connected (UMTE), Service Provider: Chunghua Telecom, Signal Strength: -102 dBm, Last Connection Up Time: 01:00:31, Tx Bytes: 302 bytes, Rx Bytes: 344 bytes, 3G Card Manufacturer: Sierra Wireless, Inc., 3G Card Model: MCR773, 3G Card Firmware Revision: H1\_1\_0\_09CAP, 3G Card IMEI: 352675011060644, SIM Card IMSI: 464922000455438.
- Latest Alerts:**

Date/Time	Message
2008-02-25 05:17:10	WAN2 connection is up.
2008-01-01 00:00:10	WAN1 connection is up.
- System Status:** Port Statistics, DNAT Table.
- WAN Interfaces:**

WAN	Status	IP Address	Subnet	Gateway	Mode	Action
WAN 1	100M/Full	123.23.23.234	255.255.255.0		DHCP client	Renew
WAN 2	Connected	133.33.33.334	255.255.255.255		IPCP client	Drop
LAN	100M/Full	192.168.1.13	255.255.255.0		DHCP server	N/A
DWZ	100M/Full	0.0.0.0/0.0.0.0			Static	N/A

### 4.5.3 Public IP Address Mapping

To have the local computers and servers use specific WAN IP addresses, you need to map static public IP addresses to them.

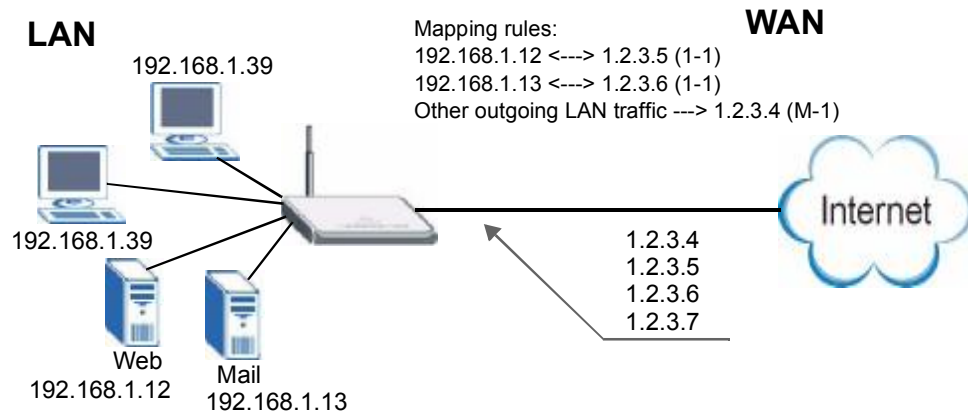


The one-to-one NAT address mapping rules are for both incoming and outgoing connections. The ZyXEL Device forwards traffic that is initiated from either the LAN or the WAN to the destination IP address.



The many-to-one or many-to-many NAT address mapping rules are for outgoing connections only. That means only traffic initiated from the LAN or returned packets are allowed to go through the ZyXEL Device.

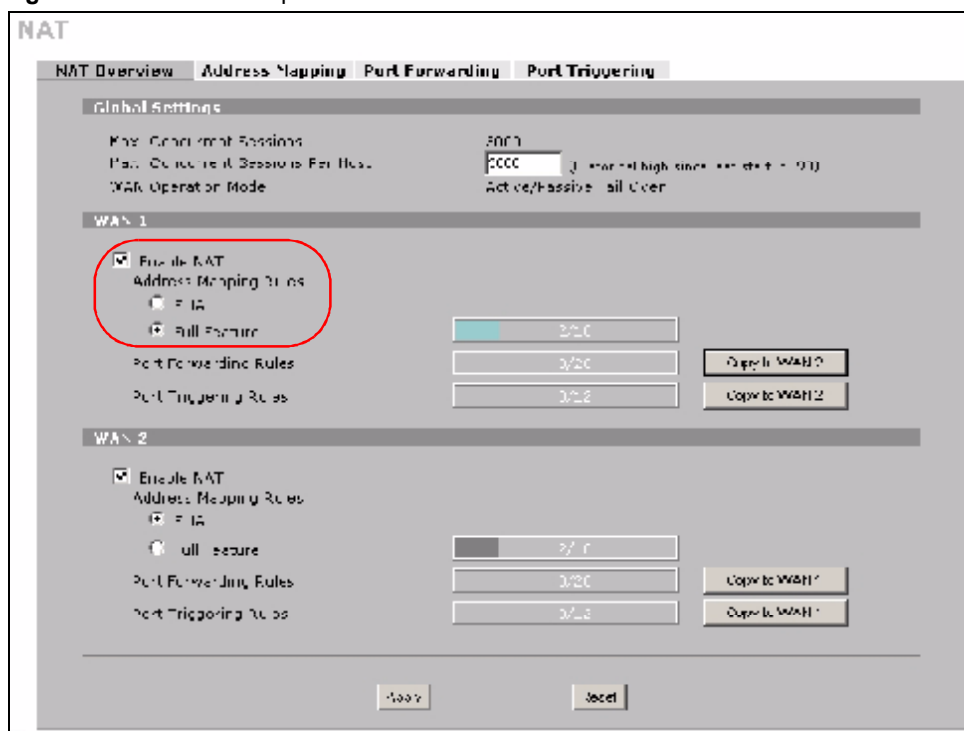
In this example, you create two one-to-one rules to map the internal web server (192.168.1.12) and mail server (192.168.1.13) to different static public IP addresses. The many-to-one rule maps a public IP address (1.2.3.4, that is, the ZyXEL Device's WAN 1 IP address) to outgoing LAN traffic. It allows other local computers on the same subnet as the ZyXEL Device's LAN IP address to use this IP address to access the Internet.

**Figure 43** Tutorial Example: Mapping Multiple Public IP Addresses to Inside Servers

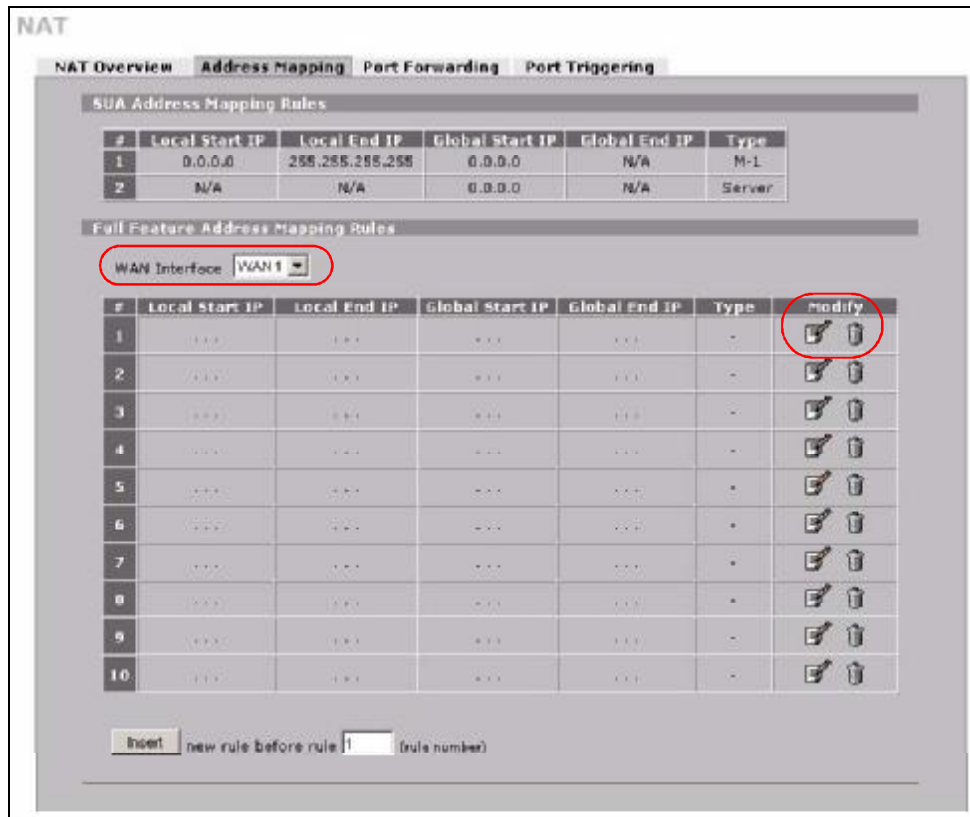
The ZyXEL Device applies the rules in the order that you specify. You should put any one-to-one rules before a many-to-one rule.

- 1 Click **ADVANCED** > **NAT**.
- 2 Enable NAT and select **Full Feature** for the WAN 1 interface as you have multiple public IP addresses to map to private IP addresses. Click **Apply**.

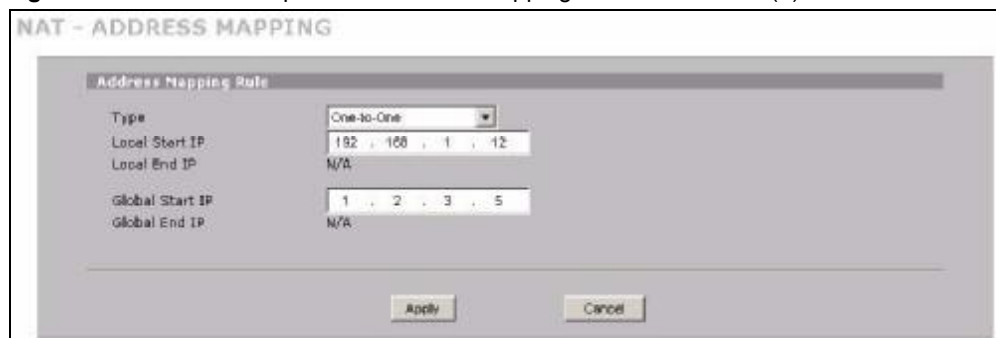
Figure 44 Tutorial Example: NAT &gt; NAT Overview



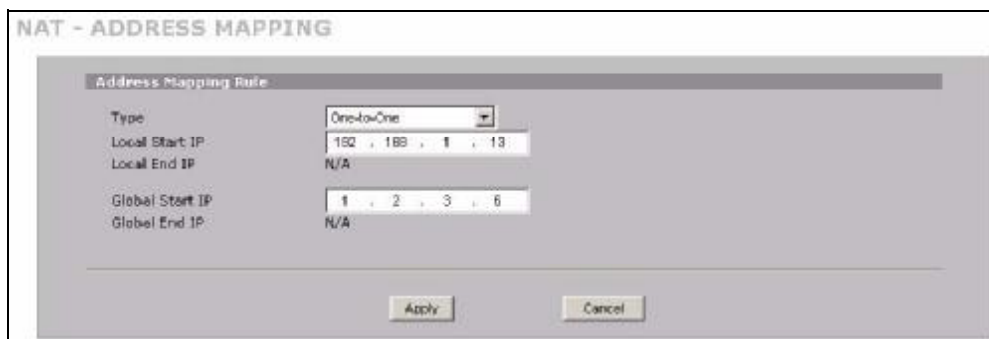
- 3 Click the **Address Mapping** tab.
- 4 Select **WAN 1**.
- 5 Click the first rule's **Edit** icon (✎) in the **Modify** column to display the **Address Mapping Rule** screen.

**Figure 45** Tutorial Example: NAT > Address Mapping

- Map a public IP address to the web server.  
Select the **One-to-One** type and enter 192.168.1.12 as the local start IP address and 1.2.3.5 as the global start IP address. Click **Apply**.

**Figure 46** Tutorial Example: NAT Address Mapping Edit: One-to-One (1)

- Click the second rule's **Edit** icon (✎).
- Map a public IP address to the mail server.  
Select the **One-to-One** type and enter 192.168.1.13 as the local start IP address and 1.2.3.6 as the global start IP address. Click **Apply**.

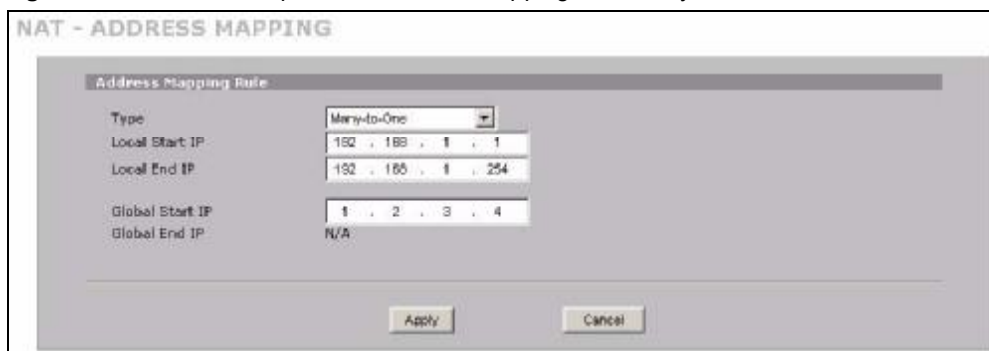
**Figure 47** Tutorial Example: NAT Address Mapping Edit: One-to-One (2)

The screenshot shows the 'NAT - ADDRESS MAPPING' configuration window. The 'Address Mapping Rule' section is active. The 'Type' is set to 'One-to-One'. The 'Local Start IP' is '192 . 168 . 1 . 13' and the 'Local End IP' is 'N/A'. The 'Global Start IP' is '1 . 2 . 3 . 6' and the 'Global End IP' is 'N/A'. There are 'Apply' and 'Cancel' buttons at the bottom.

9 Click the third rule's **Edit** icon (✎).

10 Map a public IP address to other outgoing LAN traffic.

Select the **Many-to-One** type and enter 192.168.1.1 as the local start IP address, 192.168.1.254 as the local end IP address and 1.2.3.4 as the global start IP address. Click **Apply**.

**Figure 48** Tutorial Example: NAT Address Mapping Edit: Many-to-One

The screenshot shows the 'NAT - ADDRESS MAPPING' configuration window. The 'Address Mapping Rule' section is active. The 'Type' is set to 'Many-to-One'. The 'Local Start IP' is '192 . 168 . 1 . 1' and the 'Local End IP' is '192 . 168 . 1 . 254'. The 'Global Start IP' is '1 . 2 . 3 . 4' and the 'Global End IP' is 'N/A'. There are 'Apply' and 'Cancel' buttons at the bottom.

11 After the configurations, the **Address Mapping** screen looks as shown. You still have one IP address (1.2.3.7) that can be assigned to another internal server when you expand your network.

Figure 49 Tutorial Example: NAT Address Mapping Done

NAT





















NAT Overview Address Mapping Port Forwarding Port Triggering

SUA Address Mapping Rules

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1	0.0.0.0	255.255.255.255	0.0.0.0	N/A	M-1
2	N/A	N/A	0.0.0.0	N/A	Server

FEL Feature Address Mapping Rules

WAN Interface: WAN1

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168.1.12	N/A	1.2.3.5	N/A	1-1	 
2	192.168.1.13	N/A	1.2.3.6	N/A	1-1	 
3	192.168.1.1	192.168.1.254	1.2.3.4	N/A	M-1	 
4	...	...	...	...	-	 
5	...	...	...	...	-	 
6	...	...	...	...	-	 
7	...	...	...	...	-	 
8	...	...	...	...	-	 
9	...	...	...	...	-	 
10	...	...	...	...	-	 

Insert new rule before rule 1 (rule number)



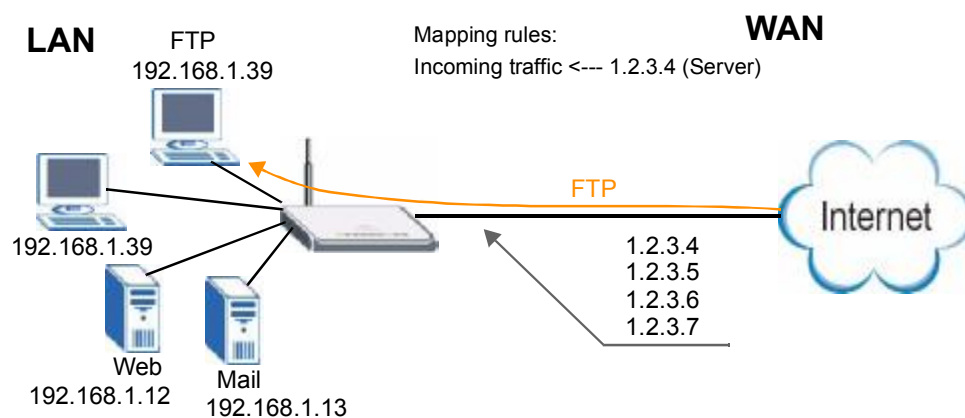
To allow traffic from the WAN to be forwarded through the ZyXEL Device, you must also create a firewall rule. Refer to [Section 4.5.5 on page 89](#) for more information.

#### 4.5.4 Forwarding Traffic from the WAN to a Local Computer

A server NAT address mapping rule allows computers behind the NAT be accessible to the outside world. To have the ZyXEL Device forward incoming traffic to a specific computer on your local network, you should also create a port forwarding (server mapping) rule.

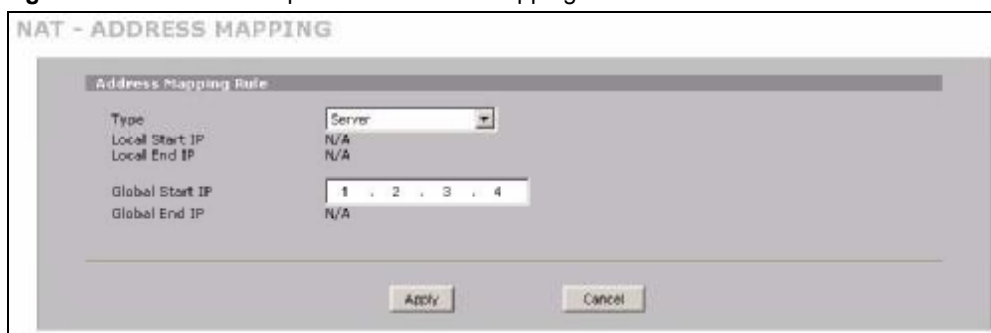
In this example, you want to forward FTP traffic using port 21 to the computer with the IP address of 192.168.1.39.

**Figure 50** Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer



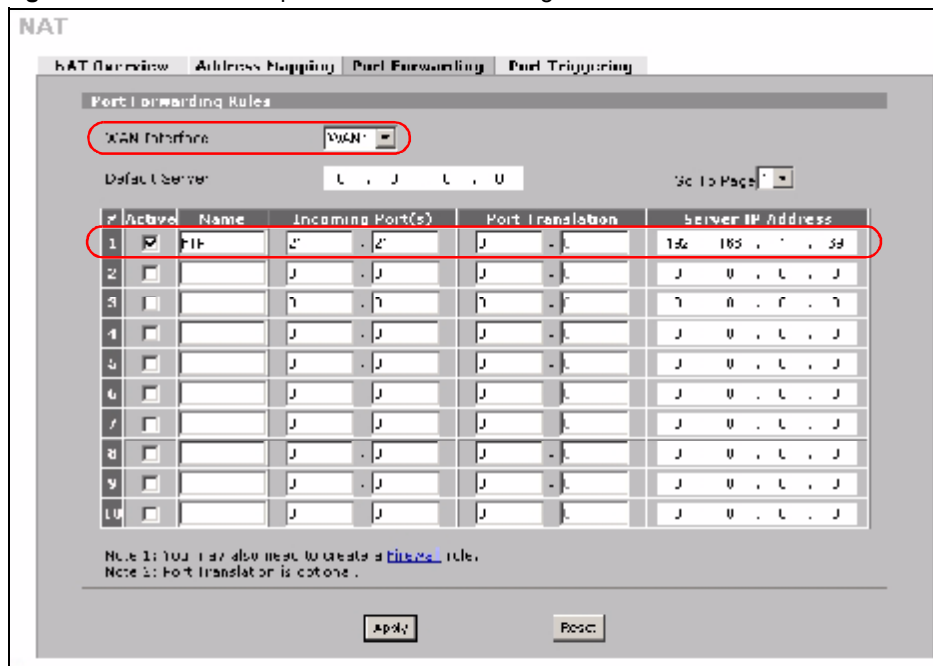
- 1 Click **ADVANCED** > **NAT** > **Address Mapping**.
- 2 Click the forth rule's **Edit** icon (✎) to configure a server rule.

**Figure 51** Tutorial Example: NAT Address Mapping Edit: Server



- 3 Click the **Port Forwarding** tab.
- 4 Select **WAN 1**.
- 5 Select the **Active** check box, enter a descriptive name (**FTP** for example), incoming port number (21) and 192.168.1.39 as the server IP address. Click **Apply**.



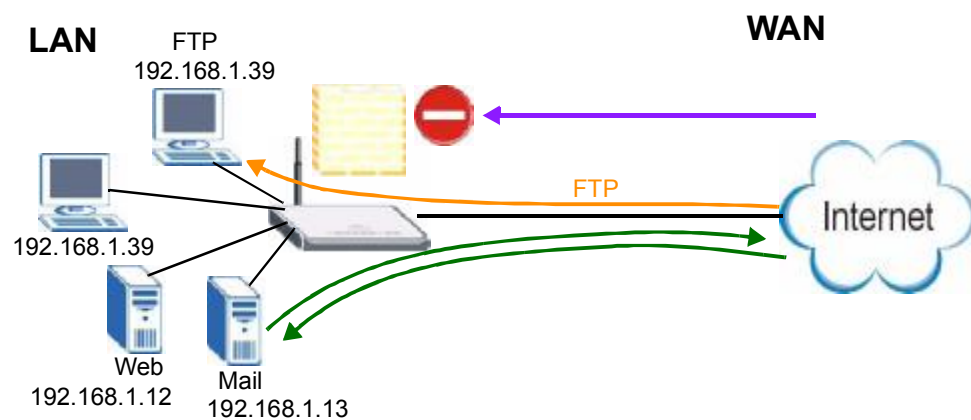
**Figure 52** Tutorial Example: NAT Port Forwarding

#### 4.5.5 Allow WAN-to-LAN Traffic through the Firewall

By default, the ZyXEL Device blocks any traffic initiated from the WAN to the LAN. To have the ZyXEL Device forward traffic initiated from WAN 1 to a local computer or server on the LAN, you need to configure a firewall rule to allow it.

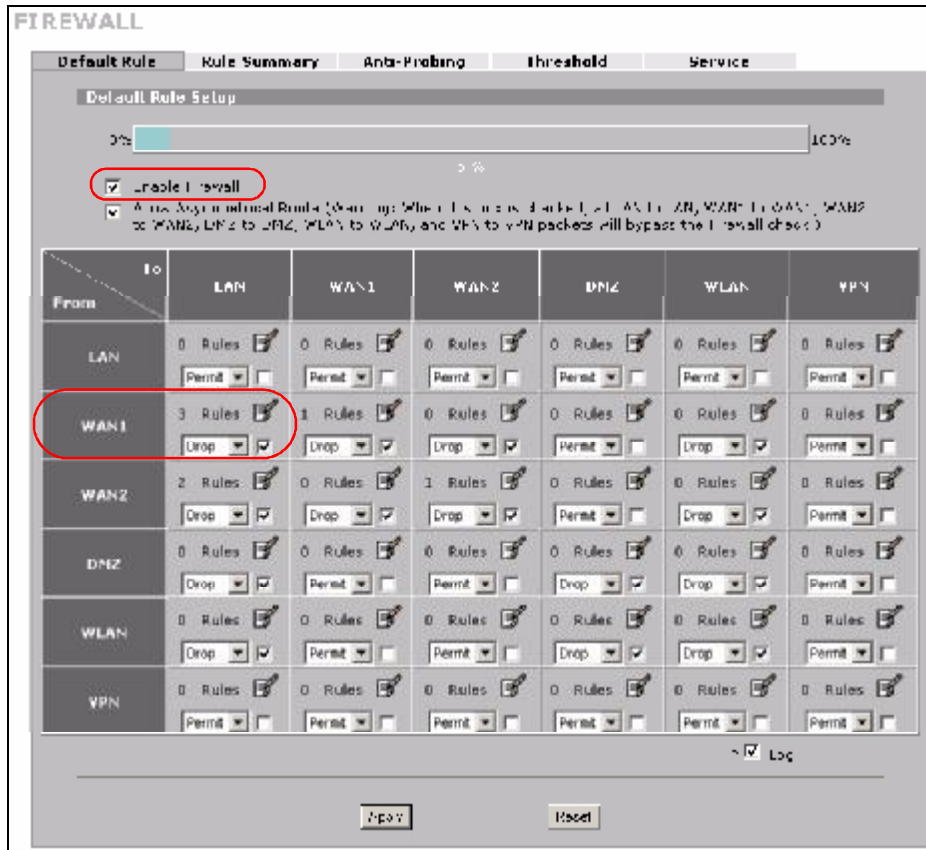
In this example, you create the firewall rules to allow traffic from the WAN to the following servers on the LAN:

- Web server
- Mail server
- FTP server

**Figure 53** Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer

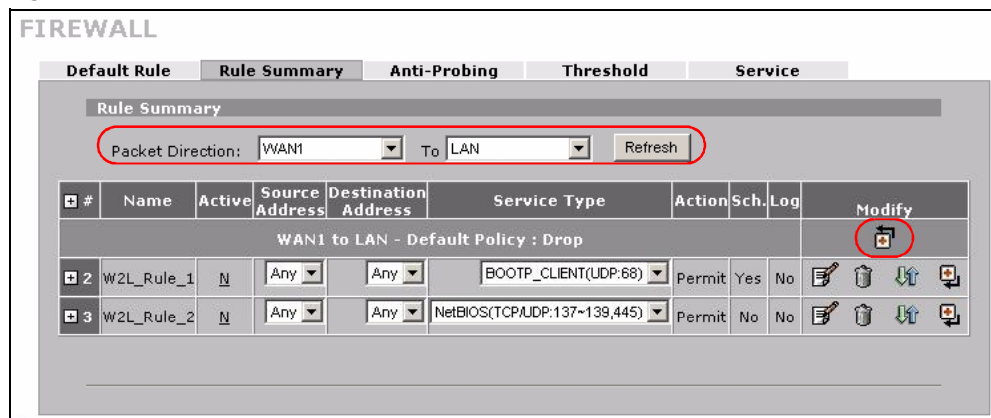
- 1 Click **SECURITY > FIREWALL**.
- 2 Make sure the firewall is enabled and traffic from WAN 1 to the LAN is dropped.

**Figure 54** Tutorial Example: Firewall Default Rule



- 3 Go to the **Rule Summary** screen.
- 4 Select **WAN1** to **LAN** as the packet direction and click **Refresh**.
- 5 Click the insert icon to create a new firewall rule.

**Figure 55** Tutorial Example: Firewall Rule: WAN1 to LAN



- 6 Configure a firewall rule to allow HTTP traffic from the WAN to the web server.  
 Enter a descriptive name (W-L\_Web for example).  
 Select **Any** in the **Destination Address(es)** box and click **Delete**.  
 Select **Single Address** as the destination address type. Enter 192.168.1.12 and click **Add**.

**Figure 56** Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Web Server

The screenshot shows the 'FIREWALL - EDIT RULE' configuration interface. The 'Rule Name' field is highlighted with a red circle and contains the text 'W-L\_Web'. Below this, there are two main sections: 'Edit Source Address' and 'Edit Destination Address'. In the 'Edit Source Address' section, the 'Address Type' is set to 'Any Address' and the 'Destination Address(es)' box contains 'Any'. In the 'Edit Destination Address' section, the 'Address Type' is set to 'Single Address' and the 'Start IP Address' field contains '192.168.1.12'. The 'Edit Service' section is partially visible at the bottom of the window.

- 7 Select **HTTP(TCP:80)** and **HTTPS(TCP:443)** in the **Available Services** box on the left, and click >> to add them to the **Selected Service(s)** box on the right. Click **Apply**.

**Figure 57** Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Web Server

**Edit Service**

Available Services (See [Service](#))

- BOOTP\_CLIENT(UDP:68)
- BOOTP\_SERVER(UDP:67)
- CU-SEEME(TCP/UDP:7648,24032)
- DNS(TCP/UDP:53)
- FINGER(TCP:79)
- FTP(TCP:20,21)
- H.323(TCP:1720)
- IAX/IAX2(UDP:4569)
- ICQ(UDP:4000)
- IKE(UDP:500)
- IMAP(TCP:143)
- IMAP3(TCP:220)
- IMAPS(TCP:993)
- IPSEC\_TRANSPORT/TUNNEL(AH:0)
- IPSEC\_TUNNEL(ESP:0)

Selected Service(s)

- HTTP(TCP:80)
- HTTPS(TCP:443)

**Edit Schedule**

Day to Apply:

Sun  Mon  Tue  Wed  Thu  Fri  Sat

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

All day

Start:  (Hour)  (Minute) End:  (Hour)  (Minute)

**Actions When Matched**

Log Packet Information When Matched

Send Alert Message to Administrator When Matched

Action for Matched Packets:

- 8 Click the insert icon to configure a firewall rule to allow traffic from the WAN to the mail server.

Enter a descriptive name (W-L\_Mail for example).

Select **Any** in the **Destination Address(es)** box and click **Delete**.

Select **Single Address** as the destination address type. Enter 192.168.1.13 and click **Add**.

**Figure 58** Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Mail Server

**FIREWALL - EDIT RULE**

Rule Name: MCL\_Mail

**Edit Source Address**

Address Editor: Any Address  
 Address Type: Any Address  
 Start IP Address: 0 . 0 . 0 . 0  
 End IP Address: 0 . 0 . 0 . 0  
 Subnet Mask: 0 . 0 . 0 . 0  
 Add Modify Delete

**Edit Destination Address**

Address Editor: Single Address  
 Address Type: Single Address  
 Start IP Address: 192 . 168 . 1 . 13  
 End IP Address: 0 . 0 . 0 . 0  
 Subnet Mask: 0 . 0 . 0 . 0  
 Add Modify Delete

**Edit Service**

- 9** Select **Any(All)** in the **Available Services** box on the left, and click >> to add it to the **Selected Service(s)** box on the right. Click **Apply**.

**Figure 59** Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Mail Server

**Edit Service**

Available Services: (See [Service](#))

Any(TCP)  
 Any(UDP)  
 Any(ICMP)  
 AMNEW\_ICG(TCP:5190)  
 AUTH(TCP:113)  
 BGP(TCP:179)  
 BOOTP\_CLIENT(UDP:68)  
 BOOTP\_SERVER(UDP:67)  
 CU-SEBME(TCP:UDP:7648,24032)  
 DNS(TCP:UDP:53)  
 FINGER(TCP:79)  
 FTP(TCP:20,21)  
 H.323(TCP:1720)  
 HTTP(TCP:80)  
 HTTPS(TCP:443)

Selected Service(s): Any(All)

**Edit Schedule**

Day to Apply:  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

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

**Actions When Matched**

Log Packet Information When Matched  
 Send Alert Message to Administrator When Matched  
 Action for Matched Packets: Permit

Apply Cancel

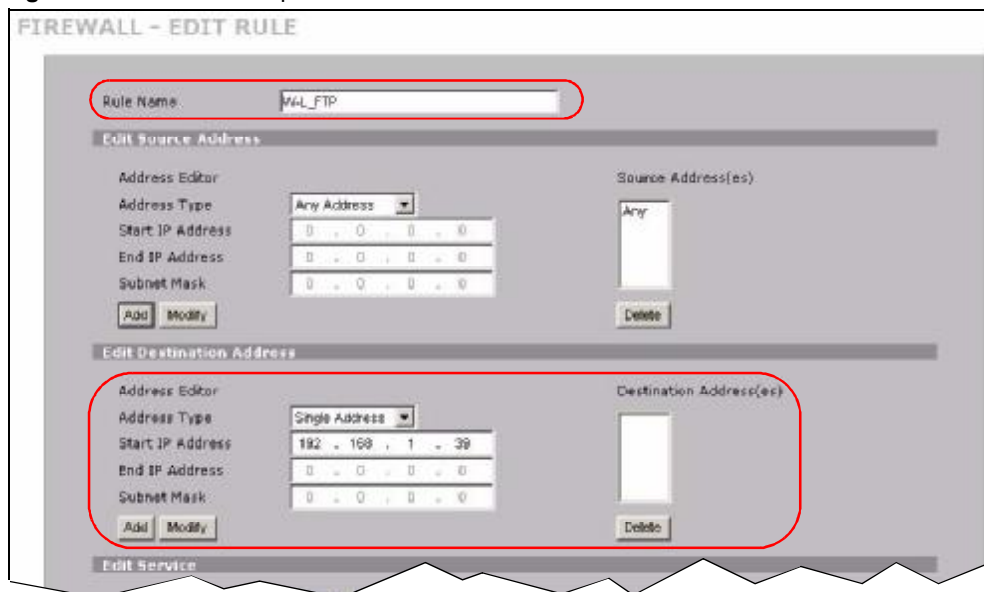
- 10 Click the insert icon to configure a firewall rule to allow FTP traffic from the WAN to the FTP server.

Enter a descriptive name (W-L\_FTP for example).

Select **Any** in the **Destination Address(es)** box and click **Delete**.

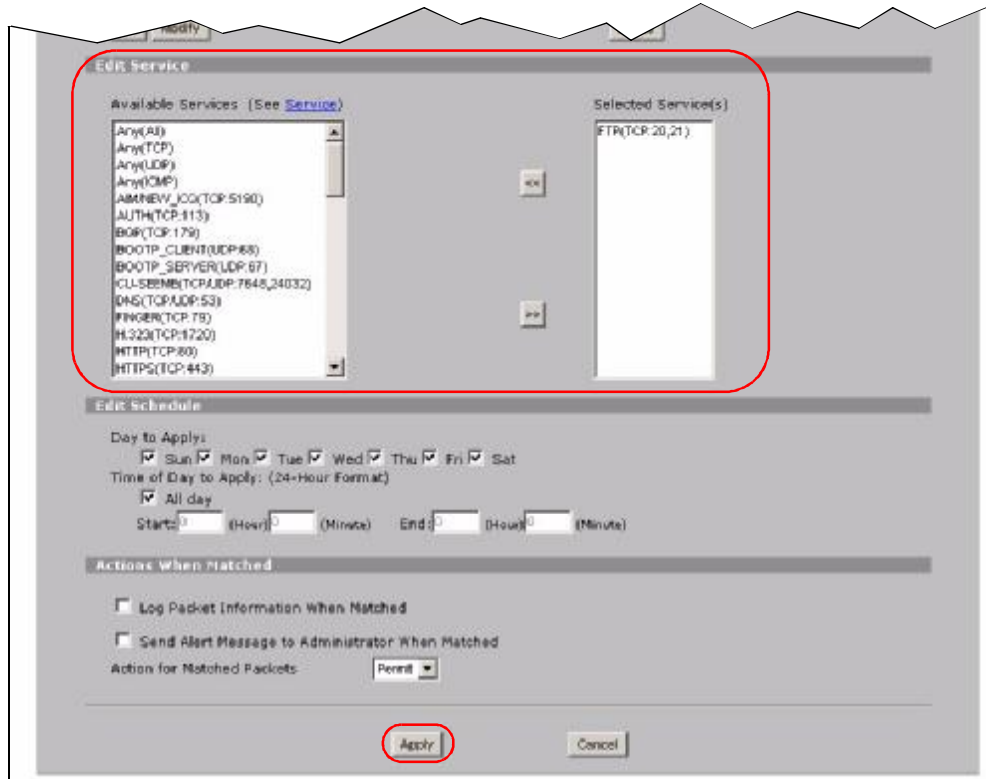
Select **Single Address** as the destination address type. Enter 192.168.1.39 and click **Add**.

**Figure 60** Tutorial Example: Firewall Rule: WAN to LAN Address Edit for FTP Server



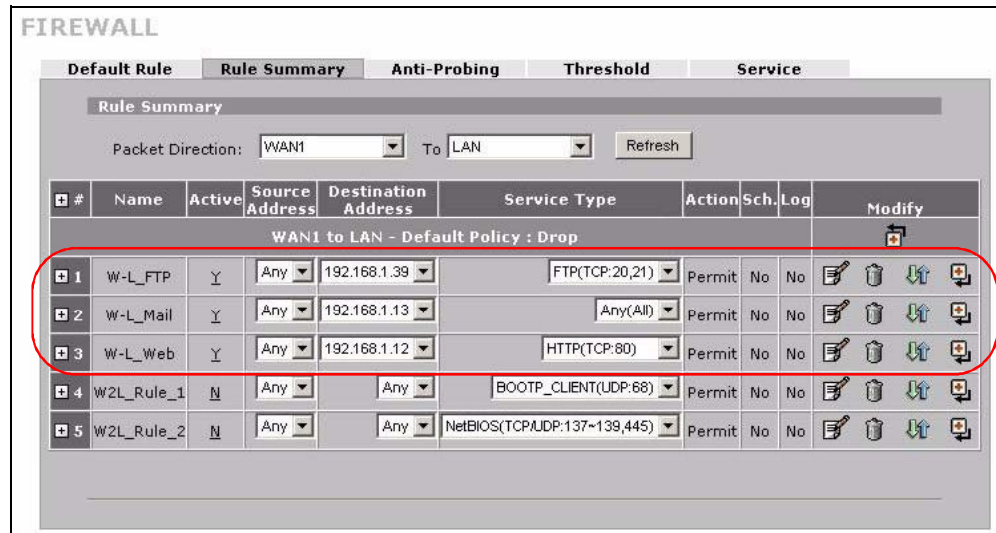
- 11 Select **FTP(TCP:20,21)** in the **Available Services** box on the left, and click >> to add it to the **Selected Service(s)** box on the right. Click **Apply**.

**Figure 61** Tutorial Example: Firewall Rule: WAN to LAN Service Edit for FTP Server



**12** When you are done, the **Rule Summary** screen looks as shown.

**Figure 62** Tutorial Example: Firewall Rule Summary



### 4.5.6 Testing the Connections

- 1 Open the web browser on one of the local computers and enter any web site's URL in the address bar. If you can access the web site, your WAN 1 connection and NAT address mapping are configured successfully. If you cannot access it, make sure you entered the correct information in the **WAN** and **NAT Address Mapping** screens. Also check that the Internet account is active and the computer's IP address is in the same subnet as the ZyXEL Device.
- 2 Open your web browser and try accessing the web server (1.2.3.5) from the outside network. If you cannot access the web server, make sure the NAT address mapping rule is configured correctly and there is a firewall rule to allow HTTP traffic from the WAN to the web server.
- 3 Try accessing the FTP server (1.2.3.4) from the outside network to send or retrieve a file. If you cannot access the FTP server, make sure the NAT port forwarding rule is active and there is a firewall rule to allow FTP traffic from the WAN to FTP server.

## 4.6 Using NAT with Multiple Game Players

If two users (behind the ZyXEL Device) want to connect to the same server to play online games at the same time, but the server does not allow more than one login from the same IP address, you can configure a many-to-many rule instead of a many-to-one rule.

In this example, you have four static IP addresses (1.2.3.4 to 1.2.3.7) from your ISP. After you set up your WAN connection (see [Section 4.5.2 on page 78](#)), use the **NAT > Address Mapping** screen to map the third and fourth public IP addresses to the mail server (192.168.1.12) and web server (192.168.1.13) respectively. The first and second public IP addresses are mapped to other outgoing LAN traffic. See [Section 4.5.3 on page 82](#) for more information about IP address mapping.

When you finish configuration, the screen looks as shown.



**Figure 63** Tutorial Example: NAT Address Mapping Done: Game Playing

NAT

NAT Overview **Address Mapping** Port Forwarding Port Triggering

SUA Address Mapping Rules

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1	0.0.0.0	255.255.255.255	0.0.0.0	N/A	M-1
2	N/A	N/A	0.0.0.0	N/A	Server

Full Feature Address Mapping Rules

WAN Interface: WAN1

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168.1.12	N/A	1.2.3.6	N/A	1-1	
2	192.168.1.13	N/A	1.2.3.7	N/A	1-1	
3	192.168.1.1	192.168.1.254	1.2.3.4	1.2.3.5	M-M Ov	
4	...	...	...	...	-	
5	...	...	...	...	-	
6	...	...	...	...	-	
7	...	...	...	...	-	
8	...	...	...	...	-	
9	...	...	...	...	-	
10	...	...	...	...	-	

Insert new rule before rule 1 (rule number)



To allow traffic from the WAN to be forwarded through the ZyXEL Device, you must also create a firewall rule. Refer to [Section 4.5.5 on page 89](#) for more information.



---

# PART II

## Network

---

LAN Screens (101)

WAN Screens (111)

DMZ Screens (135)



# LAN Screens

This chapter describes how to configure LAN settings.

## 5.1 LAN, WAN and the ZyXEL Device

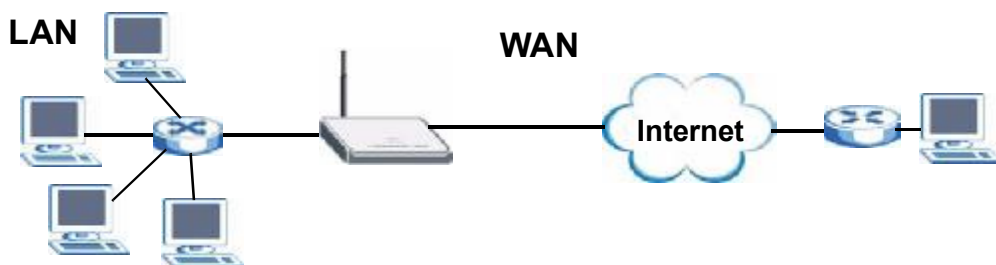
A network is a shared communication system to which many computers are attached.

The Local Area Network (LAN) includes the computers and networking devices in your home or office that you connect to the ZyXEL Device's LAN ports.

The Wide Area Network (WAN) is another network (most likely the Internet) that you connect to the ZyXEL Device's WAN port. See [Chapter 6 on page 111](#) for how to use the WAN screens to set up your WAN connection.

The LAN and the WAN are two separate networks. The ZyXEL Device controls the traffic that goes between them. The following graphic gives an example.

**Figure 64** LAN and WAN



## 5.2 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. If you select 192.168.1.0 as the network number; it 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.

### 5.2.1 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.



---

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*.

---

### 5.3 DHCP

The ZyXEL Device can use DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) to automatically assign IP addresses subnet masks, gateways, and some network information like the IP addresses of DNS servers to the computers on your LAN. You can alternatively have the ZyXEL Device relay DHCP information from another DHCP server. If you disable the ZyXEL Device's DHCP service, you must have another DHCP server on your LAN, or else the computers must be manually configured.

### 5.3.1 IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the computers on your LAN. See [Chapter 22 on page 345](#) for the default IP pool range. Do not assign your LAN computers static IP addresses that are in the DHCP pool.

## 5.4 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. 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** 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** send 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 **RIP Version** to **RIP-1**.

## 5.5 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.

## 5.6 WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

## 5.7 LAN

Click **NETWORK > LAN** to open the **LAN** screen. Use this screen to configure the ZyXEL Device's IP address and other LAN TCP/IP settings as well as the built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

**Figure 65** NETWORK > LAN

The screenshot shows the LAN configuration interface. It includes sections for LAN TCP/IP settings (IP Address, Subnet Mask, Multicast, IP Direction, RIP Version), DHCP Setup (DHCP mode, Sharing Address, Server Address, WINS Servers), and Windows Networking options (NetBIOS over TCP/IP). The interface is designed for web-based configuration with various input fields and dropdown menus.



The following table describes the labels in this screen.

**Table 12** NETWORK > LAN

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your ZyXEL Device in dotted decimal notation. 192.168.1.1 is the factory default. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyXEL Device will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received. <b>Both</b> is the default.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Multicast	Select <b>IGMP V-1</b> or <b>IGMP V-2</b> or <b>None</b> . 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 <i>sections 4 and 5 of RFC 2236</i> .
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to <b>Server</b> . When configured as a server, the ZyXEL Device provides TCP/IP configuration for the clients. When set as a server, fill in the <b>IP Pool Starting Address</b> and <b>Pool Size</b> fields. Select <b>Relay</b> to have the ZyXEL Device forward DHCP requests to another DHCP server. When set to <b>Relay</b> , fill in the <b>DHCP Server Address</b> field. Select <b>None</b> to stop the ZyXEL Device from acting as a DHCP server. When you select <b>None</b> , you must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Server Address	Type the IP address of the DHCP server to which you want the ZyXEL Device to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.

**Table 12** NETWORK > LAN (continued)

LABEL	DESCRIPTION
DHCP WINS Server 1, 2	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
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 WAN1	Select this check box to forward NetBIOS packets from the LAN to WAN 1 and from WAN 1 to the LAN. If your firewall is enabled with the default policy set to block WAN 1 to LAN traffic, you also need to enable the default WAN 1 to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to WAN 1 and from WAN 1 to the LAN.
Allow between LAN and WAN2	Select this check box to forward NetBIOS packets from the LAN to WAN 2 and from WAN 2 to the LAN. If your firewall is enabled with the default policy set to block WAN 2 to LAN traffic, you also need to enable the default WAN 2 to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to WAN 2 and from WAN 2 to the LAN.
Allow between LAN and DMZ	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.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 5.8 LAN Static DHCP

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 > Static DHCP**. The screen appears as shown.

Figure 66 NETWORK &gt; LAN &gt; Static DHCP

The screenshot shows the 'Static DHCP Table' configuration screen. It features a table with 32 rows and three columns: '#', 'MAC Address', and 'IP Address'. The 'IP Address' column contains the default value '0.0.0.0' for each row. Below the table are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 13 NETWORK &gt; LAN &gt; Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your LAN.
IP Address	Type the IP address that you want to assign to the computer on your LAN. Alternatively, click the right mouse button to copy and/or paste the IP address.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 5.9 LAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The ZyXEL Device has a single LAN interface. Even though more than one of ports 1~4 may be in the LAN port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

The ZyXEL Device supports three logical LAN interfaces via its single physical LAN Ethernet interface. The ZyXEL Device itself is the gateway for each of the logical LAN networks.

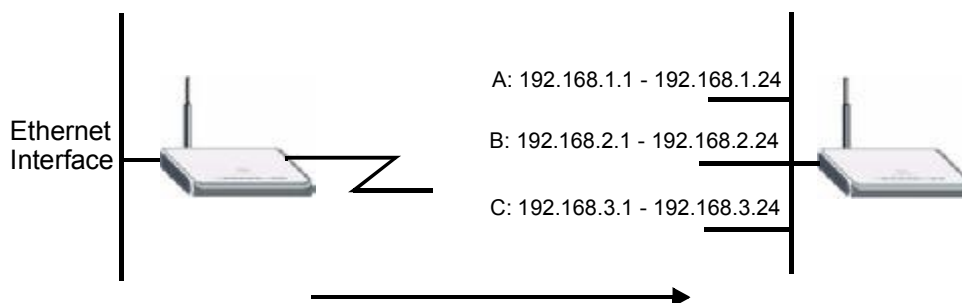
When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).



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

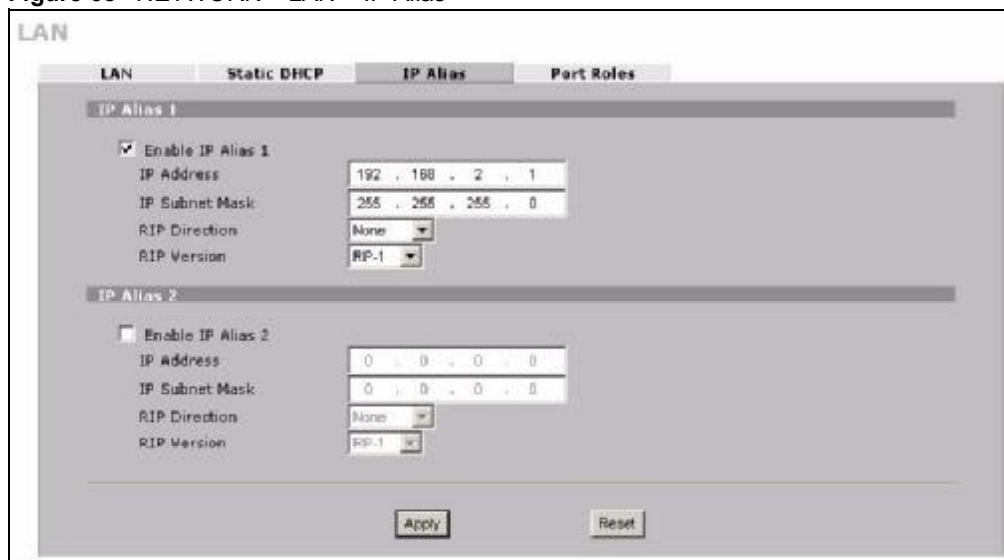
The following figure shows a LAN divided into subnets A, B, and C.

**Figure 67** 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 68** NETWORK > LAN > IP Alias



The following table describes the labels in this screen.

**Table 14** NETWORK > LAN > IP Alias

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

## 5.10 LAN Port Roles

Use the **Port Roles** screen to set ports as part of the LAN or DMZ interface.

Ports 1~4 on the ZyXEL Device can be part of the LAN or DMZ interface.



Do the following if you are configuring from a computer connected to a LAN or DMZ port and changing the port's role:

- 1 A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyXEL Device's LAN or DMZ IP address.
- 2 Use the appropriate LAN or DMZ IP address to access the ZyXEL Device.

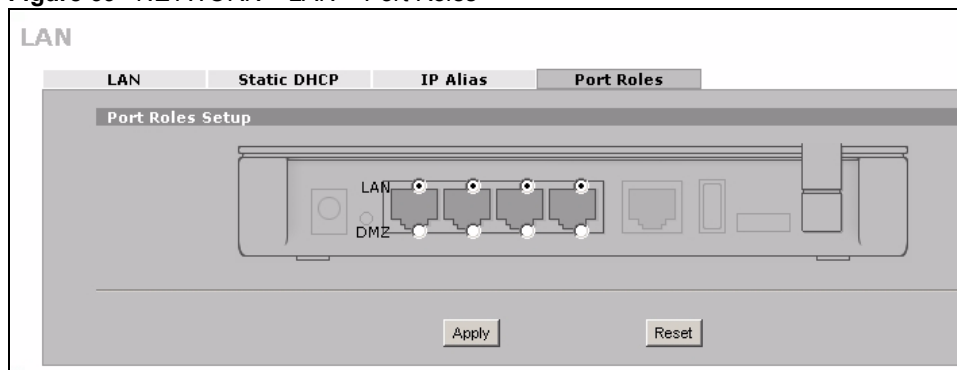
To change your ZyXEL Device's port role settings, click **NETWORK > LAN > Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyXEL Device. On the ZyXEL Device, ports 1 to 4 are all LAN ports by default.



Your changes are also reflected in the **DMZ Port Roles** screen.

**Figure 69** NETWORK > LAN > Port Roles



The following table describes the labels in this screen.

**Table 15** NETWORK > LAN > Port Roles

LABEL	DESCRIPTION
LAN	Select a port's LAN radio button to use the port as part of the LAN. The port will use the ZyXEL Device's LAN IP address and MAC address.
DMZ	Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the ZyXEL Device's DMZ IP address and MAC address.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

After you change the LAN or DMZ port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

**Figure 70** Port Roles Change Complete



# WAN Screens

This chapter describes how to configure WAN settings.



---

WAN 2 refers to the 3G card on the supported ZyXEL Device.

---

## 6.1 WAN Overview

- Use the **WAN General** screen to configure operation mode, route priority and connection test for the ZyXEL Device.
- Use the **WAN 1** screen to configure the WAN1 interface for Internet access on the ZyXEL Device.
- Use the **3G (WAN 2)** screen to configure the WAN2 interface for Internet access on the ZyXEL Device.
- Use the **Traffic Redirect** screen to configure an alternative gateway.

## 6.2 Multiple WAN

You can use a second connection as a backup to enhance network reliability.

The ZyXEL Device has two WAN ports. You can optionally activate the internal 3G card to use the second 3G WAN interface. You can connect one interface to one ISP (or network) and connect the other to a second ISP (or network).

The ZyXEL Device's NAT feature allows you to configure sets of rules for one WAN interface and separate sets of rules for the other WAN interface. Refer to [Chapter 12 on page 225](#) for details.

You can select through which WAN interface you want to send out traffic from UPnP-enabled applications (see [Chapter 16 on page 281](#)).

The ZyXEL Device's DDNS lets you select which WAN interface you want to use for each individual domain name. The DDNS high availability feature lets you have the ZyXEL Device use the other WAN interface for a domain name if the configured WAN interface's connection goes down. See [Section 14.10.2 on page 256](#) for details.

### 6.3 TCP/IP Priority (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".

- 1 The metric sets the priority for the ZyXEL Device's routes to the Internet. Each route must have a unique metric.
- 2 The priorities of the WAN interface routes must always be higher than the traffic redirect route priorities.

Lets say that you have the WAN operation mode set to active/passive, meaning the ZyXEL Device use the second highest priority WAN interface as a back up. The WAN 1 route has a metric of "2", the WAN 2 route has a metric of "3", and the traffic-redirect route has a metric of "14". In this case, the WAN 1 route acts as the primary default route. If the WAN 1 route fails to connect to the Internet, the ZyXEL Device tries the WAN 2 route next. If the WAN 2 route fails, the ZyXEL Device tries the traffic-redirect route.

The traffic redirect route cannot take priority over the WAN 1 and WAN 2 routes.

### 6.4 WAN General

Click **NETWORK > WAN** to open the **General** screen. Use this screen to configure operation mode, route priority and connection test.



---

WAN 2 refers to the 3G card on the supported ZyXEL Device.

---



Figure 71 NETWORK &gt; WAN General

**WAN**

**General** | WAN 1 | 3G (WAN 2) | Traffic Redirect

**Operation Mode**

Active/Passive (Fail Over) Mode  
 Fall Back to Primary WAN When Possible

**Route Priority**

WAN	Priority (metric)	1(Highest) ~ 15(Lowest)
WAN 1	1	1(Highest) ~ 15(Lowest)
WAN 2	2	1(Highest) ~ 15(Lowest)
Traffic Redirect	14	1(Highest) ~ 15(Lowest)

**Connectivity Check**

Check Period: 5 (5 ~ 300 (Seconds))  
 Check Timeout: 3 (1 ~ 10 (Seconds))  
 Check Fail Tolerance: 3 (1 ~ 10 (Successive Checks))

Check WAN 1 Connectivity  
 Ping Default Gateway: 129.23.23.254  
 Ping this Address: [ ] (Domain Name or IP Address)

Check WAN 2 Connectivity  
 Ping Default Gateway: 0.0.0.0  
 Ping this Address: [ ] (Domain Name or IP Address)

Check Traffic Redirection Connectivity  
 Ping Default Gateway: 0.0.0.0  
 Ping this Address: [ ] (Domain Name or IP Address)

**Windows Networking (NetBIOS over TCP/IP)**

Allow between WAN1 and LAN  
 Allow between WAN1 and DMZ  
 Allow between WAN2 and LAN  
 Allow between WAN2 and DMZ  
 Allow Trigger Dial

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

Apply Reset

The following table describes the labels in this screen.

**Table 16** NETWORK > WAN General

LABEL	DESCRIPTION
Active/Passive (Fail Over) Mode	The ZyXEL Device uses the second highest priority WAN interface as a back up. This means that the ZyXEL Device will normally use the highest priority (primary) WAN interface (depending on the priorities you configure in the <b>Route Priority</b> fields). The ZyXEL Device will switch to the secondary (second highest priority) WAN interface when the primary WAN interface's connection fails.
Fall Back to Primary WAN When Possible	This field determines the action the ZyXEL Device takes after the primary WAN interface fails and the ZyXEL Device starts using the secondary WAN interface. Select this check box to have the ZyXEL Device change back to using the primary WAN interface when the ZyXEL Device can connect through the primary WAN interface again. Clear this check box to have the ZyXEL Device continue using the secondary WAN interface, even after the ZyXEL Device can connect through the primary WAN interface again. The ZyXEL Device continues to use the secondary WAN interface until it's connection fails (at which time it will change back to using the primary WAN interface if its connection is up).
Route Priority	
WAN1 WAN2 Traffic Redirect	The default WAN connection is "1" as your broadband connection via the WAN interface should always be your preferred method of accessing the WAN. The ZyXEL Device switches from WAN interface 1 to WAN interface 2 if WAN interface 1's connection fails and then back to WAN interface 1 when WAN interface 1's connection comes back up. The default priority of the routes is <b>WAN 1</b> , <b>WAN 2</b> and then <b>Traffic Redirect</b> : You have two choices for an auxiliary connection ( <b>WAN 2</b> and <b>Traffic Redirect</b> ) in the event that your regular WAN connection goes down.
Connectivity Check	
Check Period	The ZyXEL Device tests a WAN connection by periodically sending a ping to either the default gateway or the address in the <b>Ping this Address</b> field. Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Check Timeout	Type the number of seconds (1 to 10) for your ZyXEL Device to wait for a response to the ping before considering the check to have failed. This setting must be less than the <b>Check Period</b> . Use a higher value in this field if your network is busy or congested.
Check Fail Tolerance	Type how many WAN connection checks can fail (1-10) before the connection is considered "down" (not connected). The ZyXEL Device still checks a "down" connection to detect if it reconnects.
Check WAN1/2 Connectivity	Select the check box to have the ZyXEL Device periodically test the respective WAN interface's connection. Select <b>Ping Default Gateway</b> to have the ZyXEL Device ping the WAN interface's default gateway IP address. Select <b>Ping this Address</b> and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the ZyXEL Device ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.

**Table 16** NETWORK > WAN General (continued)

LABEL	DESCRIPTION
Check Traffic Redirection Connectivity	<p>Select the check box to have the ZyXEL Device periodically test the traffic redirect connection.</p> <p>Select <b>Ping Default Gateway</b> to have the ZyXEL Device ping the backup gateway's IP address.</p> <p>Select <b>Ping this Address</b> and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the ZyXEL Device ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.</p>
Windows Networking (NetBIOS over TCP/IP)	<p>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.</p>
Allow between WAN1 and LAN	<p>Select this check box to forward NetBIOS packets from WAN 1 to the LAN port and from the LAN port to WAN1. If your firewall is enabled with the default policy set to block WAN 1 to LAN traffic, you also need to enable the default WAN1 to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from WAN 1 to the LAN port and from LAN port to WAN1.</p>
Allow between WAN1 and DMZ	<p>Select this check box to forward NetBIOS packets from WAN 1 to the DMZ port and from the DMZ port to WAN1.</p> <p>Clear this check box to block all NetBIOS packets going from WAN 1 to the DMZ port and from DMZ port to WAN1.</p>
Allow between WAN2 and LAN	<p>Select this check box to forward NetBIOS packets from WAN 2 to the LAN port and from the LAN port to WAN2. If your firewall is enabled with the default policy set to block WAN 2 to LAN traffic, you also need to enable the default WAN2 to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from WAN 2 to the LAN port and from LAN port to WAN2.</p>
Allow between WAN2 and DMZ	<p>Select this check box to forward NetBIOS packets from WAN 2 to the DMZ port and from the DMZ port to WAN2.</p> <p>Clear this check box to block all NetBIOS packets going from WAN 2 to the DMZ port and from DMZ port to WAN2.</p>
Allow Trigger Dial	<p>Select this option to allow NetBIOS packets to initiate calls.</p>
Apply	<p>Click <b>Apply</b> to save your changes.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 6.5 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, 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.

**Table 17** Private IP Address Ranges

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 have it assigned by 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.



---

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.

---

## 6.6 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of [www.zyxel.com](http://www.zyxel.com) is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyXEL Device can get the DNS server addresses in the following ways.

- 1 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, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the ZyXEL Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- 3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see [Section 14.5.1 on page 248](#)).

## 6.7 WAN MAC Address

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 can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

## 6.8 WAN 1

Use this screen to change your ZyXEL Device's WAN 1 ISP, IP and MAC settings. Click **NETWORK > WAN > WAN 1** to display this screen. The screen differs by the encapsulation.



The WAN 1 and WAN 2 IP addresses of a ZyXEL Device with multiple WAN interfaces must be on different subnets.

### 6.8.1 WAN Ethernet Encapsulation

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyXEL Device** firewall rule for those packets. Contact your ISP to find the correct port number.

The screen shown next is for **Ethernet** encapsulation.

**Figure 72** NETWORK > WAN > WAN 1 (Ethernet Encapsulation)

**WAN**

General **WAN 1** 3G (WAN 2) Traffic Redirect

**ISP Parameters for Internet Access**

Encapsulation: Ethernet

Service Type: RRR-Toshiba

User Name: [ ]

Password: [ ]

Retype to Confirm: [ ]

Login Server IP Address: 0 . 0 . 0 . 0

**WAN IP Address Assignment**

Get Automatically from ISP

Use Fixed IP Address

My WAN IP Address: 0 . 0 . 0 . 0

My WAN IP Subnet Mask: 0 . 0 . 0 . 0

Gateway IP Address: 0 . 0 . 0 . 0

**Advanced Setup**

Enable NAT (Network Address Translation)

RIP Direction: None

RIP Version: RIPv1

Enable Multicast

Multicast Version: IGMPv1

Spoof WAN MAC Address from LAN

Clone the computer's MAC address - IP Address: 192 . 168 . 1 . 33

Apply Reset

The following table describes the labels in this screen.

**Table 18** NETWORK > WAN > WAN 1 (Ethernet Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet.
Service Type	Choose from <b>Standard</b> , <b>Telstra</b> (RoadRunner Telstra authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method), <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method) or <b>Telia Login</b> . The following fields do not appear with the <b>Standard</b> service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one. This field is not available for Telia Login.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example login1.telia.com.
Relogin Every(min) (Telia Login only)	The Telia server logs the ZyXEL Device out if the ZyXEL Device does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyXEL Device to wait between logins.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
My WAN IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Advanced Setup	
Enable NAT (Network Address Translation)	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). Select this check box to enable NAT.

**Table 18** NETWORK > WAN > WAN 1 (Ethernet Encapsulation) (continued)

LABEL	DESCRIPTION
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the ZyXEL Device will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the ZyXEL Device will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving).</p> <p>Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that 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, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>
Enable Multicast	<p>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.</p>
Multicast Version	<p>Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b>. IGMP (Internet Group Multicast Protocol) is a session-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.</p>
Spoof WAN MAC Address from LAN	<p>You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the ZyXEL Device uses the factory assigned MAC Address to identify itself on the WAN.</p> <p>Otherwise, select the check box next to <b>Spoof WAN MAC Address from LAN</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.</p>
Clone the computer's MAC address – IP Address	<p>Enter the IP address of the computer on the LAN whose MAC you are cloning. If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port.</p>
Apply	<p>Click <b>Apply</b> to save your changes.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 6.8.2 PPPoE Encapsulation

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

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

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

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

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

The screen shown next is for **PPPoE** encapsulation.



**Figure 73** NETWORK > WAN > WAN 1 (PPPoE Encapsulation)

The following table describes the labels in this screen.

**Table 19** NETWORK > WAN > WAN 1 (PPPoE Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select <b>PPPoE</b> for a dial-up connection using PPPoE.
Service Name	Type the PPPoE service name provided to you by your ISP. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.

**Table 19** NETWORK > WAN > WAN 1 (PPPoE Encapsulation) (continued)

LABEL	DESCRIPTION
Authentication Type	<p>The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.</p> <p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p><b>CHAP/PAP</b> - Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node.</p> <p><b>CHAP</b> - Your ZyXEL Device accepts CHAP only.</p> <p><b>PAP</b> - Your ZyXEL Device accepts PAP only.</p>
Nailed-Up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyXEL Device automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option if the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
Advanced Setup	
Enable NAT (Network Address Translation)	<p>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).</p> <p>Select this checkbox to enable NAT.</p> <p>For more information about NAT see <a href="#">Chapter 12 on page 225</a>.</p>
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the ZyXEL Device will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the ZyXEL Device will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that 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, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>

**Table 19** NETWORK > WAN > WAN 1 (PPPoE Encapsulation) (continued)

LABEL	DESCRIPTION
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 Version	Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b> . IGMP (Internet Group Multicast Protocol) is a session-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.
Spoof WAN MAC Address from LAN	You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the ZyXEL Device uses the factory assigned MAC Address to identify itself on the WAN. Otherwise, select the check box next to <b>Spoof WAN MAC Address from LAN</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Clone the computer's MAC address – IP Address	Enter the IP address of the computer on the LAN whose MAC you are cloning. If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 6.8.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The screen shown next is for **PPTP** encapsulation.

**Figure 74** NETWORK > WAN > WAN 1 (PPTP Encapsulation)

The screenshot shows the WAN configuration interface for WAN 1. It includes the following sections and fields:

- ISP Parameters for Internet Access:** Encapsulation (PPTP), User Name, Password, Retype to Confirm, Authentication Type (CHAP/PAP), Nailed-Up checkbox, and Idle Timeout (100 seconds).
- PPTP Configuration:** My IP Address, My IP Subnet Mask, Server IP Address, and Connection ID/Name.
- WAN IP Address Assignment:** Radio buttons for 'Get Automatically from ISP' (selected) and 'Use Fixed IP Address' (with a field for My WAN IP Address).
- Advanced Setup:** 'Enable NAT (Network Address Translation)' checkbox (checked), RIP Direction (None), RIP Version (RIPv1), 'Enable Multicast' checkbox (unchecked) with Multicast Version (IGMPv1), and 'Spoof WAN MAC Address from LAN' checkbox (unchecked) with a field for 'Clone the computer's MAC address - IP Address' (192.168.1.33).

The following table describes the labels in this screen.

**Table 20** NETWORK > WAN > WAN 1 (PPTP Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Set the encapsulation method to <b>PPTP</b> . The ZyXEL Device supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.

**Table 20** NETWORK > WAN > WAN 1 (PPTP Encapsulation) (continued)

LABEL	DESCRIPTION
Authentication Type	<p>The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.</p> <p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p><b>CHAP/PAP</b> - Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node.</p> <p><b>CHAP</b> - Your ZyXEL Device accepts CHAP only.</p> <p><b>PAP</b> - Your ZyXEL Device accepts PAP only.</p>
Nailed-up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyXEL Device automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My 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.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option if the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
Advanced Setup	
Enable NAT (Network Address Translation)	<p>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).</p> <p>Select this checkbox to enable NAT.</p> <p>For more information about NAT see <a href="#">Chapter 12 on page 225</a>.</p>
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the ZyXEL Device will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the ZyXEL Device will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>

**Table 20** NETWORK > WAN > WAN 1 (PPTP Encapsulation) (continued)

LABEL	DESCRIPTION
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving).</p> <p>Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that 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, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>
Enable Multicast	<p>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.</p>
Multicast Version	<p>Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b>. IGMP (Internet Group Multicast Protocol) is a session-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.</p>
Spoof WAN MAC Address from LAN	<p>You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the ZyXEL Device uses the factory assigned MAC Address to identify itself on the WAN.</p> <p>Otherwise, select the check box next to <b>Spoof WAN MAC Address from LAN</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.</p>
Clone the computer's MAC address – IP Address	<p>Enter the IP address of the computer on the LAN whose MAC you are cloning. If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port.</p>
Apply	<p>Click <b>Apply</b> to save your changes.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 6.9 3G (WAN 2)

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.



The actual data rate you obtain varies depending on your 3G card, the signal strength of the service provider's base station, your service plan, etc.

If the signal strength of a 3G network is too low, the 3G card may switch to an available 2.5G or 2.75G network. See the following table for a comparison between 2G, 2.5G, 2.75G, 3G and 3.5G wireless technologies.

**Table 21** 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies

NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio. CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.		
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU <sup>A</sup> specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		

A. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

After you activate 3G on your ZyXEL Device, the 3G connection becomes WAN 2. Refer to the [Chapter 22 on page 345](#) for the type of 3G cards that you can use in the ZyXEL Device along with the corresponding supported features.

To change your ZyXEL Device's 3G WAN settings, click **NETWORK > WAN > 3G (WAN 2)** or **WIRELESS > 3G (WAN 2)**.



The WAN 1 and WAN 2 IP addresses of a ZyXEL Device with multiple WAN interfaces must be on different subnets.

**Figure 75** NETWORK > WAN > 3G (WAN 2)

**WAN**

General | WAN 1 | **3G (WAN 2)** | Traffic Redirect

**WAN2 Setup**

Enable

**3G Card Configuration**

3G Interface: USB Slot[01] - SIERRA WIRELESS AIRCARD 8775 \* Device will reboot after chan

Network Type: Automatically (All bands)

Network Selection: Automatically Scan \* Scan takes about 30 secs

**ISP Parameters for Internet Access**

Access Point Name (APN): internet

Initial String (containing APN): at&fs0=0

Authentication Type: None

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Retype to Confirm: \_\_\_\_\_

PIN Code: 0000

Phone Number: \*99#

Nailed-Up

Idle Timeout: 100 (Seconds)

**WAN IP Address Assignment**

Get Automatically from ISP

Use Fixed IP Address

My WAN IP Address: 0 . 0 . 0 . 0

**Advanced Setup**

Enable NAT (Network Address Translation)

Enable Multicast

Multicast Version: IGMP-v1

Enable Budget Control

Time Budget: 0 hours per month

Data Budget: 0 Mbytes Download/Upload per month

Reset time and data budget counters on last day of each month

Reset time and data budget counters

**Actions when over budget**

Log  Alert  recurring every 0 minute(s)

Allow  Disallow New 3G connection

Keep  Drop Current 3G connection

Actions when over 0 % of time budget or 0 % of data budget

Log  Alert  recurring every 0 minute(s)

Apply Reset



The following table describes the labels in this screen.

**Table 22** NETWORK > WAN > 3G (WAN 2)

LABEL	DESCRIPTION
WAN2 Setup	
Enable	Select this option to enable WAN 2. The <b>Network Type</b> and <b>Network Selection</b> fields appear.
3G Card Configuration	
3G Interface	This displays the model of the 3G card installed in your ZyXEL Device.
Network Type	<p>Select the type of 3G service and frequency band for your 3G connection. If you are unsure what to select, check with your 3G service provider to find the 3G service available to you in your region.</p> <p>Select <b>Automatically (All bands)</b> to have the card connect to the highest speed network available. Once connected the ZyXEL Device will continue searching for and connecting to the highest speed network as it becomes available.</p> <p>Select <b>UMTS/HSDPA only (WCDMA 2100)</b> to access HSDPA or UMTS networks available at 2100 Mhz in your region. At the time of writing, Europe and Asia offer UMTS or HSDPA using WCDMA 2100.</p> <p>Select <b>GPRS/EDGE (GSM 900/1800) only</b> to access GPRS or EDGE networks available at 900 or 1800 Mhz in your region. At the time of writing, Europe and most of Asia offer GPRS or EDGE using GSM 900/1800. GSM 1800 may also be known as DCS in some countries.</p> <p>Select <b>GSM all</b> to access GPRS or EDGE networks in other GSM frequency bands in other regions.</p> <p>Select <b>WCDMA all</b> to access UMTS or HSDPA networks in other WCDMA frequency bands in other regions.</p> <p>See <a href="#">Table 21 on page 127</a> for more information.</p>
Network Selection	<p>Select a 3G service provider for your connection. Otherwise, select <b>Automatically</b> to have the ZyXEL Device use the default settings on the 3G SIM card and connect to your service provider's base station.</p> <p>This shows <b>Automatically</b> by default. Click <b>Scan</b> to have the ZyXEL Device search for and display the available service providers. Ensure you have disconnected your 3G connection as the ZyXEL Device cannot scan for available 3G service providers while it has a 3G connection.</p> <p>This field resets to the default setting (<b>Automatically</b>) if the ZyXEL Device restarts.</p>
ISP Parameters for Internet Access	
Access Point Name (APN)	<p>Select this option and enter the APN (Access Point Name) if your ISP gives you the APN only. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge methods.</p> <p>You can enter up to 31 ASCII printable characters. Spaces are allowed.</p>
Initial String (containing APN)	<p>Select this option and enter the initial string and APN if you know how to configure or your ISP provides a string, which would include the APN, to initialize the 3G card.</p> <p>You can enter up to 72 ASCII printable characters. Spaces are allowed.</p>

**Table 22** NETWORK > WAN > 3G (WAN 2) (continued)

LABEL	DESCRIPTION
Authentication Type	<p>The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.</p> <p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p><b>CHAP/PAP</b> - Your ZyXEL Device accepts either CHAP or PAP when requested by the ISP.</p> <p><b>CHAP</b> - Your ZyXEL Device accepts CHAP only.</p> <p><b>PAP</b> - Your ZyXEL Device accepts PAP only.</p> <p><b>None</b> - Your ZyXEL Device does not send your user name and password for authentication. The user name and password fields are grayed out. Select this option if your ISP did not give you a user name and password.</p>
User Name	Type the user name (of up to 31 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 31 ASCII printable characters) associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
PIN Code	<p>A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card.</p> <p>Enter the PIN code (four to eight digits, 0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet.</p> <p>If your ISP disabled PIN code authentication, enter an arbitrary number.</p> <p>This field is available only when you insert a GSM 3G card.</p> <p>Check the <b>HOME</b> screen to see if you have entered the correct PIN.</p>
Phone Number	<p>Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the dial string.</p> <p>By default, *99# is the dial string for GSM-based networks and #777 is the dial string for CDMA-based networks.</p>
Nailed-Up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	This specifies the time (from 0 to 9999) in seconds that elapses before the ZyXEL Device automatically disconnects from the ISP.
WAN IP Address Assignment	
Get automatically from ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option if the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
Advanced Setup	
Enable NAT (Network Address Translation)	<p>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).</p> <p>Select this checkbox to enable NAT.</p> <p>For more information about NAT see <a href="#">Chapter 12 on page 225</a>.</p>

**Table 22** NETWORK > WAN > 3G (WAN 2) (continued)

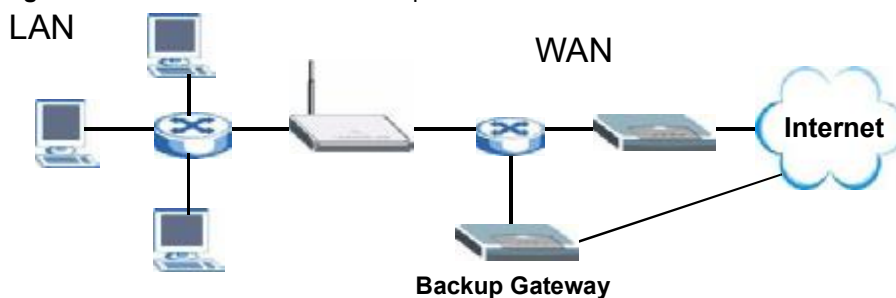
LABEL	DESCRIPTION
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b> . IGMP (Internet Group Multicast Protocol) is a session-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.
Enable Budget Control	Select this check box to set a monthly limit for the user account of the installed 3G card. You must insert a 3G card before you enable budget control on the ZyXEL Device. You can set a limit on the total traffic and/or call time. The ZyXEL Device takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this check box and specify the amount of time (in hours) that the 3G connection can be used within one month. If you change the value after you configure and enable budget control, the ZyXEL Device resets the statistics.
Data Budget	Select this check box and specify how much downstream and/or upstream data (in Mbytes) can be transmitted via the 3G connection within one month. Select <b>Download</b> to set a limit on the downstream traffic (from the ISP to the ZyXEL Device). Select <b>Upload</b> to set a limit on the upstream traffic (from the ZyXEL Device to the ISP). Select <b>Download/Upload</b> to set a limit on the total traffic in both directions. If you change the value after you configure and enable budget control, the ZyXEL Device resets the statistics.
Reset time and data budget counters on	Select the date on which the ZyXEL Device resets the budget every month. If the date you selected is not available in a month, such as 30th or 31th, the ZyXEL Device resets the budget on the last day of the month.
Reset time and data budget counters	This button is available only when you enable budget control in this screen. Click this button to reset the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart.
Actions when over budget	Specify the actions the ZyXEL Device takes when the time or data limit is exceeded. Select <b>Log</b> to create a log. Select <b>Alert</b> to create an alert. This option is available only when you select <b>Log</b> . If you select <b>Log</b> , you can also select <b>recurring every</b> to have the ZyXEL Device send a log (and alert if selected) for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log (and alert if selected). Select <b>Allow</b> to permit new 3G connections or <b>Disallow</b> to drop/block new 3G connections. Select <b>Keep</b> to maintain the existing 3G connection or <b>Drop</b> to disconnect it. You cannot select <b>Allow</b> and <b>Drop</b> at the same time. If you select <b>Disallow</b> and <b>Keep</b> , the ZyXEL Device allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.

**Table 22** NETWORK > WAN > 3G (WAN 2) (continued)

LABEL	DESCRIPTION
Actions when over % of time budget or % of data budget	Specify the actions the ZyXEL Device takes when the specified percentage of time budget or data limit is exceeded. Enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the ZyXEL Device resets the statistics. Select <b>Log</b> to create a log. Select <b>Alert</b> to create an alert. This option is available only when you select <b>Log</b> . If you select <b>Log</b> , you can also select <b>recurring every</b> to have the ZyXEL Device send a log (and alert if selected) for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log (and alert if selected).
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

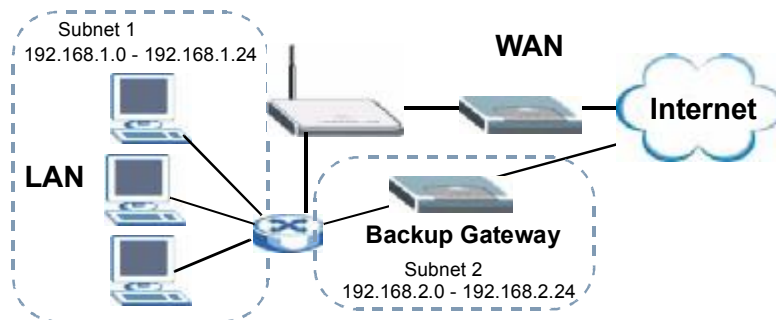
## 6.10 Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyXEL Device still provides firewall protection for the LAN.

**Figure 76** Traffic Redirect WAN Setup

IP alias allows you to avoid triangle route security issues when the backup gateway is connected to the LAN or DMZ. 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 a LAN to LAN/ZyXEL Device firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

**Figure 77** Traffic Redirect LAN Setup



## 6.11 Configuring Traffic Redirect

To change your ZyXEL Device's traffic redirect settings, click **NETWORK > WAN > Traffic Redirect**. The screen appears as shown.

**Figure 78** NETWORK > WAN > Traffic Redirect

The screenshot shows the 'WAN' configuration page with the 'Traffic Redirect' tab selected. The 'Active' checkbox is unchecked. The 'Backup Gateway IP Address' field contains '0.0.0.0'. The 'Apply' and 'Reset' buttons are visible at the bottom of the configuration area.

The following table describes the labels in this screen.

**Table 23** NETWORK > WAN > Traffic Redirect

LABEL	DESCRIPTION
Active	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# DMZ Screens

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

## 7.1 DMZ

The DeMilitarized Zone (DMZ) 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(s).

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.

## 7.2 Configuring DMZ

The DMZ and the connected computers can have private or public IP addresses.

When the DMZ uses public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See [Appendix C on page 377](#) for information on IP subnetting. If you do not configure SUA NAT or any full feature NAT mapping rules for the public IP addresses on the DMZ, the ZyXEL Device will route traffic to the public IP addresses on the DMZ without performing NAT. This may be useful for hosting servers for NAT unfriendly applications (see [Chapter 12 on page 225](#) for more information).

If the DMZ computers use private IP addresses, use NAT if you want to make them publicly accessible.

Like the LAN, the ZyXEL Device can also assign TCP/IP configuration via DHCP to computers connected to the DMZ ports.

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

Figure 79 NETWORK &gt; DMZ

The following table describes the labels in this screen.

Table 24 NETWORK &gt; DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your ZyXEL Device's DMZ port in dotted decimal notation.  Note: Make sure the IP addresses of the LAN, WAN and DMZ are on separate subnets.
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 <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyXEL Device will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received. <b>Both</b> is the default.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .



**Table 24** NETWORK > DMZ (continued)

LABEL	DESCRIPTION
Multicast	Select <b>IGMP V-1</b> or <b>IGMP V-2</b> or <b>None</b> . 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 <i>sections 4 and 5 of RFC 2236</i> .
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to <b>Server</b> . When configured as a server, the ZyXEL Device provides TCP/IP configuration for the clients. When set as a server, fill in the <b>IP Pool Starting Address</b> and <b>Pool Size</b> fields. Select <b>Relay</b> to have the ZyXEL Device forward DHCP requests to another DHCP server. When set to <b>Relay</b> , fill in the <b>DHCP Server Address</b> field. Select <b>None</b> to stop the ZyXEL Device from acting as a DHCP server. When you select <b>None</b> , you must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Server Address	Type the IP address of the DHCP server to which you want the ZyXEL Device to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
DHCP WINS Server 1, 2	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Windows Networking (NetBIOS over TCP/IP)	
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 configure a 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 1	Select this check box to forward NetBIOS packets from the DMZ to WAN 1 and from WAN 1 to the DMZ. Clear this check box to block all NetBIOS packets going from the DMZ to WAN 1 and from WAN 1 to the DMZ.
Allow between DMZ and WAN 2	Select this check box to forward NetBIOS packets from the DMZ to WAN 2 and from WAN 2 to the DMZ. Clear this check box to block all NetBIOS packets going from the DMZ to WAN 2 and from WAN 2 to the DMZ.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 7.3 DMZ Static DHCP

This table allows you to assign IP addresses on the DMZ 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 on the DMZ, click **NETWORK > DMZ > Static DHCP**. The screen appears as shown.

**Figure 80** NETWORK > DMZ > Static DHCP

#	MAC Address	IP Address
1		0 . 0 . 0 . 0
2		0 . 0 . 0 . 0
3		0 . 0 . 0 . 0
4		0 . 0 . 0 . 0
5		0 . 0 . 0 . 0
6		0 . 0 . 0 . 0
7		0 . 0 . 0 . 0
8		0 . 0 . 0 . 0
9		0 . 0 . 0 . 0
10		0 . 0 . 0 . 0
11		0 . 0 . 0 . 0
12		0 . 0 . 0 . 0
13		0 . 0 . 0 . 0
14		0 . 0 . 0 . 0
15		0 . 0 . 0 . 0
16		0 . 0 . 0 . 0
17		0 . 0 . 0 . 0
18		0 . 0 . 0 . 0
19		0 . 0 . 0 . 0
20		0 . 0 . 0 . 0
21		0 . 0 . 0 . 0
22		0 . 0 . 0 . 0
23		0 . 0 . 0 . 0
24		0 . 0 . 0 . 0
25		0 . 0 . 0 . 0
26		0 . 0 . 0 . 0
27		0 . 0 . 0 . 0
28		0 . 0 . 0 . 0
29		0 . 0 . 0 . 0
30		0 . 0 . 0 . 0
31		U . U . U . U
32		0 . 0 . 0 . 0

The following table describes the labels in this screen.

**Table 25** NETWORK > DMZ > Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your DMZ.
IP Address	Type the IP address that you want to assign to the computer on your DMZ. Alternatively, click the right mouse button to copy and/or paste the IP address.

**Table 25** NETWORK > DMZ > Static DHCP

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 7.4 DMZ IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The ZyXEL Device has a single DMZ interface. Even though more than one of ports 1~4 may be in the DMZ port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

The ZyXEL Device supports three logical DMZ interfaces via its single physical DMZ Ethernet interface. The ZyXEL Device itself is the gateway for each of the logical DMZ networks.

The IP alias IP addresses can be either private or public regardless of whether the physical DMZ interface is set to use a private or public IP address. Use NAT if you want to make DMZ computers with private IP addresses publicly accessible (see [Chapter 12 on page 225](#) for more information). When you use IP alias, you can have the DMZ use both public and private IP addresses at the same time.



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

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

Figure 81 NETWORK &gt; DMZ &gt; IP Alias

The following table describes the labels in this screen.

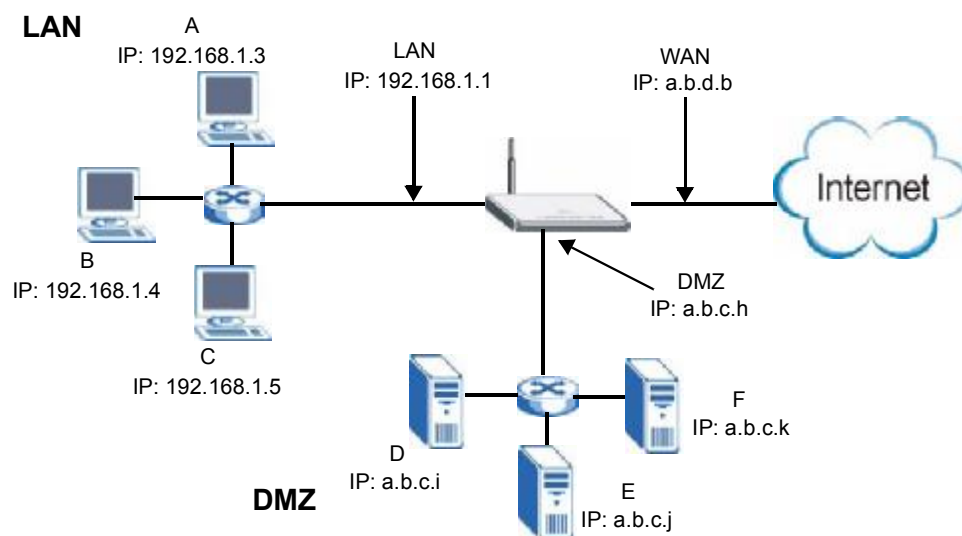
Table 26 NETWORK &gt; DMZ &gt; IP Alias

LABEL	DESCRIPTION
Enable IP Alias 1, 2	Select the check box to configure another DMZ network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation.  Note: Make sure the IP addresses of the LAN, WAN and DMZ are on separate subnets.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyXEL Device will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 7.5 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.

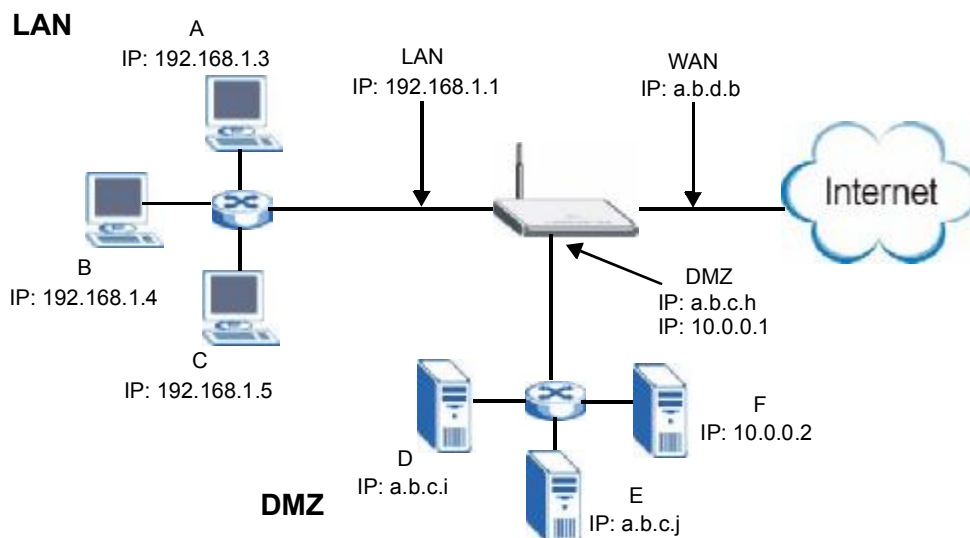
**Figure 82** DMZ Public Address Example



## 7.6 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 one subnet (either the public or the private) in the **Network > DMZ** screen (see [Figure 7.2 on page 135](#)) and configure the other subnet in the **Network > DMZ > IP Alias** screen (see [Figure 7.4 on page 139](#)) to use this kind of network setup. You also need to configure NAT for the private DMZ IP addresses.

**Figure 83** DMZ Private and Public Address Example

## 7.7 DMZ Port Roles

Use the **Port Roles** screen to set ports as part of the LAN and/or DMZ interface.

Ports 1~4 on the ZyXEL Device can be part of the LAN and/or DMZ interface.



Do the following if you are configuring from a computer connected to a LAN or DMZ port and changing the port's role:

- 1 A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyXEL Device's LAN or DMZ IP address.
- 2 Use the appropriate LAN or DMZ IP address to access the ZyXEL Device.

To change your ZyXEL Device's port role settings, click **NETWORK > DMZ > Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyXEL Device. On the ZyXEL Device, ports 1 to 4 are all LAN ports by default.



Your changes are also reflected in the **LAN Port Roles** screens.

**Figure 84** NETWORK > DMZ > Port Roles

The following table describes the labels in this screen.

**Table 27** NETWORK > DMZ > Port Roles

LABEL	DESCRIPTION
LAN	Select a port's LAN radio button to use the port as part of the LAN. The port will use the ZyXEL Device's LAN IP address and MAC address.
DMZ	Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the ZyXEL Device's DMZ IP address and MAC address.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.





---

# PART III

## Wireless

---

Wi-Fi (147)



# 8

## Wi-Fi

This chapter discusses how to configure wireless LAN on the ZyXEL Device.

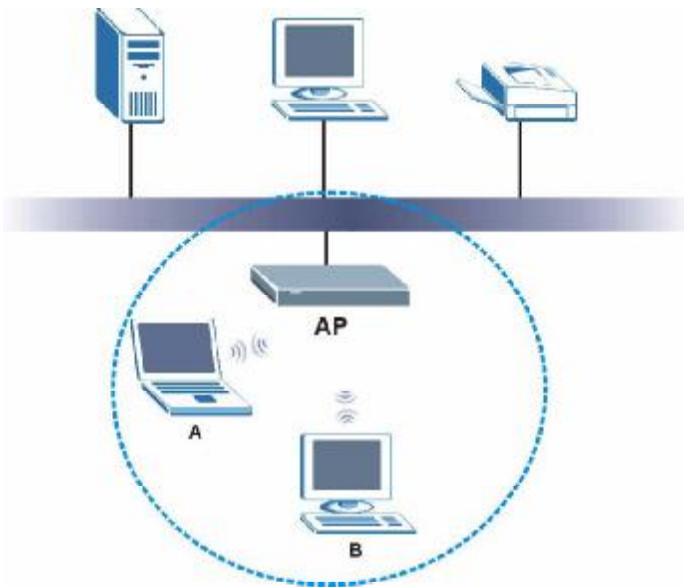
### 8.1 Wi-Fi Introduction

Your ZyXEL Device comes with an internal Wi-Fi card, providing AP (access point) functionality, and allowing you to set up a wireless LAN (WLAN). Before you set up your WLAN it is important to understand WLAN and WLAN security concepts.

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

The following figure provides an example of a wireless network.

**Figure 85** Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use different channels.

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

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

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



---

See the WLAN appendix for more detailed information on WLANs.

---

## 8.2 Wireless Security Overview

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

### 8.2.1 SSID

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

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

### 8.2.2 MAC Address Filter

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

- 
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.

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

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

### 8.2.3 User Authentication

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

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

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

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

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

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

### 8.2.4 Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See [Section 8.2.3 on page 149](#) for information about this.)

**Table 28** Types of Encryption for Each Type of Authentication

	No Authentication	RADIUS Server
Weakest	No Security	
	Static WEP	
		802.1x +Static WEP
	WPA-PSK	WPA
Strongest	WPA2-PSK or WPA2-PSK-Mix	WPA2 or WPA2-Mix

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

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



It is recommended that wireless clients use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.



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.

If some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK-Mix** or **WPA2-Mix** (depending on the type of wireless network login) in the ZyXEL Device.

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

### 8.2.5 Additional Installation Requirements for Using 802.1x

- A computer with an IEEE 802.11b/g wireless LAN card.
- A computer equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station must be running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.
- An optional network RADIUS server for remote user authentication and accounting.

## 8.3 Wireless Card

If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security 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 **WIRELESS > Wi-Fi** to open the **Wireless Card** screen.

**Figure 86** WIRELESS > Wi-Fi > Wireless Card





The following table describes the labels in this screen.

**Table 29** WIRELESS > Wi-Fi > Wireless Card

LABEL	DESCRIPTION
Enable Wireless Card	The wireless LAN through a wireless LAN card is turned off by default. Before you enable the wireless LAN you should configure security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.
Bridge to	Select <b>LAN</b> to use the wireless card as part of the LAN. Select <b>DMZ</b> to use the wireless card as part of the DMZ. The ZyXEL Device restarts after you change the wireless card setting.  Note: If you set the wireless card to be part of the LAN or DMZ, you can still use wireless access. The firewall will treat the wireless card as part of the LAN or DMZ respectively.
802.11 Mode	Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant wireless devices to associate with the ZyXEL Device. Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant wireless devices to associate with the ZyXEL Device. Select <b>802.11b+g</b> to allow both IEEE802.11b and IEEE802.11g compliant wireless devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. To have the ZyXEL Device automatically select a channel, click <b>Scan</b> instead.
Scan	Click this button to have the ZyXEL Device automatically select the wireless channel with the lowest interference.
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. <b>RTS/CTS</b> is designed to prevent collisions due to hidden nodes. You should only configure <b>RTS/CTS</b> 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. Enter a value between <b>256</b> and <b>2346</b> . Data with a frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear to Send) handshake. The lower the value, the more often the devices must get permission. If the <b>RTS/CTS</b> value is greater than the <b>Fragmentation</b> value, then the RTS/CTS handshake will never occur as data frames will be fragmented before they reach <b>RTS/CTS</b> size.
Fragmentation Threshold	This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between <b>256</b> and <b>2346</b> .
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following <b>100%</b> (full power), <b>50%</b> , <b>25%</b> , <b>12.5%</b> or <b>min</b> (minimum). See the product specifications for more information on your ZyXEL Device's output power.
Enable Roaming	Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this checkbox to enable roaming on the ZyXEL Device if you have two or more ZyXEL Devices on the same subnet.  Note: All APs on the same subnet and the wireless clients must have the same SSID to allow roaming.



**Table 29** WIRELESS > Wi-Fi > Wireless Card (continued)

LABEL	DESCRIPTION
Select SSID Profile	An SSID profile is the set of parameters relating to one of the ZyXEL Device's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a wireless client is associated. Wireless clients associating with the access point (AP) must have the same SSID.  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 security settings, you will lose your wireless connection when you press <b>Apply</b> to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
#	This field displays the index number of each SSID profile.
Active	Choose a profile to apply to your wireless network by selecting its radio button.
Name	This field displays the identification name of each SSID profile on the ZyXEL Device.
SSID	This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates which security profile is currently associated with each SSID profile. See <a href="#">Section 8.4 on page 154</a> for more information.
Action	Click the edit  icon next to the profile you want to configure and go to the SSID configuration screen. Click the reset default  icon to clear all user-entered configuration information and return the SSID profile to its factory defaults.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 8.3.1 SSID Profile

Configure wireless network security by configuring and applying an SSID profile. You can configure multiple profiles but you can only apply one to your network.

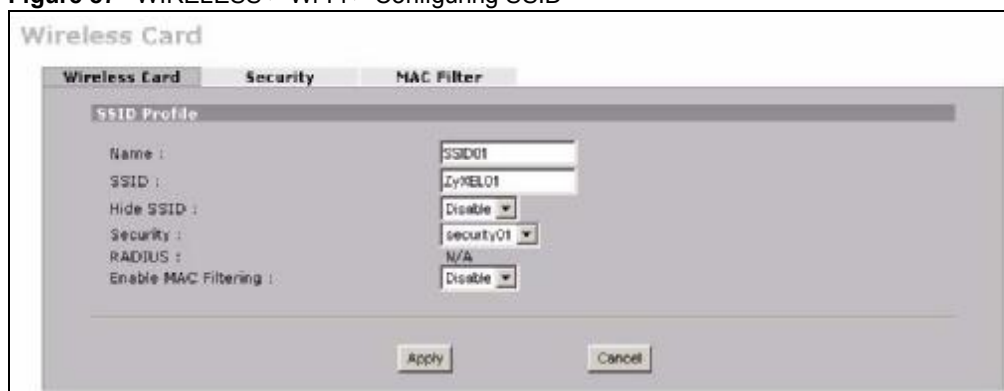
Use the **Wireless Card** screen to see information about the SSID profiles on the ZyXEL Device, and use the **Wireless Card > Edit** screen to configure the SSID profiles.

Each SSID profile references the settings configured in the following screens:

- **WIRELESS > Wi-Fi > Security** (one of the security profiles).
- **AUTH SERVER > RADIUS** (the RADIUS server settings).
- **WIRELESS > Wi-Fi > MAC Filter** (the MAC filter list, if activated in the SSID profile).

Configure the fields in the above screens to use the settings in an SSID profile.

In the **Wireless Card** screen, click the edit icon next to an SSID profile to display the following screen.

**Figure 87** WIRELESS > Wi-Fi > Configuring SSID

The following table describes the labels in this screen.

**Table 30** WIRELESS > Wi-Fi > Configuring SSID

LABEL	DESCRIPTION
Name	Enter a name (up to 32 printable 7-bit ASCII characters) identifying this profile.
SSID	When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select <b>Disable</b> if you want the ZyXEL Device to broadcast this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, select <b>Enable</b> to have the ZyXEL Device hide this SSID (a wireless client scanning for an AP will not find this SSID).
Security	Select a security profile to use with this SSID profile. See <a href="#">Section 8.4 on page 154</a> for more information.
RADIUS	This displays <b>N/A</b> if the security profile you selected does not use RADIUS authentication. See <a href="#">Section 8.4 on page 154</a> for more information. This displays <b>Radius Configuration</b> if you select a security profile that uses RADIUS authentication. Click <b>Radius Configuration</b> to go to the <b>RADIUS</b> screen where you can view and/or change the RADIUS settings. See <a href="#">Section 10.3 on page 193</a> for more information.
Enable MAC Filtering	Select <b>Enable</b> from the drop down list box to activate MAC address filtering.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 8.4 Configuring Wireless Security

Click **WIRELESS > Wi-Fi > Security** to open the **Security** screen. Use this screen to create security profiles. A security profile is a group of configuration settings which can be assigned to an SSID profile in the **Wireless Card** screen.

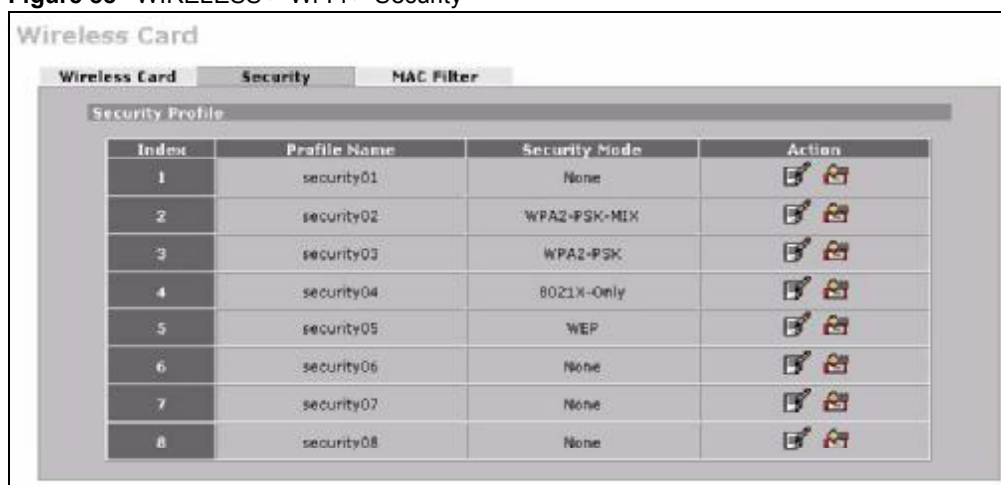
The screen changes when you configure a security profile and varies according to the security modes you select.

The following table describes the security modes you can configure.

**Table 31** Security Modes

SECURITY MODE	DESCRIPTION
None	Select this to have no data encryption.
WEP	Select this to use WEP encryption.
802.1x-Only	Select this to use 802.1x authentication with no data encryption.
802.1x-Static64	Select this to use 802.1x authentication with a static 64bit WEP key and an authentication server.
802.1x-Static128	Select this to use 802.1x authentication with a static 128bit WEP key and an authentication server.
WPA	Select this to use WPA.
WPA-PSK	Select this to use WPA with a pre-shared key.
WPA2	Select this to use WPA2.
WPA2-MIX	Select this to use either WPA2 or WPA depending on which security mode the wireless client uses.
WPA2-PSK	Select this to use WPA2 with a pre-shared key.
WPA2-PSK-MIX	Select this to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.

**Figure 88** WIRELESS > Wi-Fi > Security



The following table describes the labels in this screen.

**Table 32** WIRELESS > Wi-Fi > Security

LABEL	DESCRIPTION
Security Profile	
Index	This is the index number of the security profile.
Profile Name	This field displays a name given to a security profile in the <b>Security</b> configuration screen.
Security Mode	This field displays the security mode this security profile uses.
Action	Click the edit icon to configure security settings for that profile. Click the reset default icon to clear all user-entered configuration information and return the security profile to its factory defaults.

### 8.4.1 No Security



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

**Figure 89** WIRELESS > Wi-Fi > Security: None

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

**Table 33** WIRELESS > Wi-Fi > Security: None

LABEL	DESCRIPTION
Name	Type a name (up to 32 printable 7-bit ASCII characters) to identify this security profile.
Security Mode	Select <b>None</b> to allow wireless clients to communicate with the access points without any data encryption.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

### 8.4.2 Static WEP

Static WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data.

Your ZyXEL Device allows you to configure up to four 64-bit, 128-bit or 152-bit WEP keys, but only one key can be used at any one time.

In order to configure and enable WEP encryption, click **WIRELESS > Wi-Fi > Security > Edit**.

**Figure 90** WIRELESS > Wi-Fi > Security: WEP

**Wireless Card**

**Security Profile**

Name : security02

Security Mode : WEP

WEP Encryption : 152-bit WEP

Authentication Method : Auto

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).  
 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).  
 152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F") for each Key (1-4).  
 (Select one WEP key as an active key to encrypt wireless data transmission.)

Key 1 0x00000000000000000000000000000000

Key 2 0x00000000000000000000000000000000

Key 3 0x00000000000000000000000000000000

Key 4 0x00000000000000000000000000000000

Apply Cancel

The following table describes the labels in this screen.

**Table 34** WIRELESS > Wi-Fi > Security: WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select <b>WEP</b> from the drop-down list.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select <b>64-bit WEP</b> , <b>128-bit WEP</b> or <b>152-bit WEP</b> to enable data encryption.
Authentication Method	Select <b>Shared-Key</b> to have the ZyXEL Device use the default WEP key to authenticate the wireless client to the ZyXEL Device. Select <b>Auto</b> to have the ZyXEL Device switch between the shared-key and open system (the wireless clients and AP do not share a secret key for authentication) modes automatically. The default setting is <b>Auto</b> .
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless clients must use the same WEP key for data transmission. If you chose <b>64-bit WEP</b> in the <b>WEP Encryption</b> field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose <b>128-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose <b>152-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. You can configure up to four keys, but only one key can be activated at any one time. The default key is key 1.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

### 8.4.3 IEEE 802.1x Only

Click the **WIRELESS > Wi-Fi > Security > Edit**. Select **8021X-Only** from the **Security Mode** list.

**Figure 91** WIRELESS > Wi-Fi > Security: 802.1x Only

The following table describes the labels in this screen.

**Table 35** WIRELESS > Wi-Fi > Security: 802.1x Only

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select <b>8021X-Only</b> from the drop-down list.
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.
Authentication Databases	Click <b>Local User</b> to go to the <b>Local User Database</b> screen where you can view and/or edit the list of users and passwords. Click <b>RADIUS</b> to go to the <b>RADIUS</b> screen where you can configure the ZyXEL Device to check an external RADIUS server.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

#### 8.4.4 IEEE 802.1x + Static WEP

Click the **WIRELESS > Wi-Fi > Security > Edit**. Select **8021X-Static 64** or **8021X-Static128** in the **Security Mode** field to display the following screen.

**Figure 92** WIRELESS > Wi-Fi > Security: 802.1x + Static WEP

The following table describes the labels in this screen.

**Table 36** WIRELESS > Wi-Fi > Security: 802.1x + Static WEP

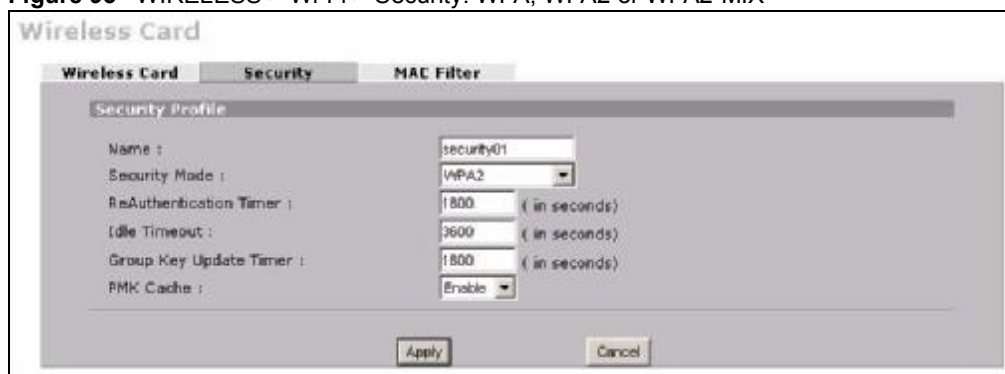
LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select <b>8021X-Static64</b> or <b>8021X-Static128</b> from the drop-down list.
Key 1 to Key 4	<p>If you chose <b>8021X-Static64</b> in the <b>Security Mode</b> field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>If you chose <b>8021X-Static128</b> in the <b>Security Mode</b> field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless clients.</p>
ReAuthentication Timer	<p>Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds.</p> <p>If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Idle Timeout	<p>The ZyXEL Device automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.</p> <p>This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again.</p> <p>Enter a time interval between 600 and 65535 seconds.</p>
Authentication Databases	Click <b>Local User</b> to go to the <b>Local User Database</b> screen where you can view and/or edit the list of users and passwords. Click <b>RADIUS</b> to go to the <b>RADIUS</b> screen where you can configure the ZyXEL Device to check an external RADIUS server.

**Table 36** WIRELESS > Wi-Fi > Security: 802.1x + Static WEP (continued)

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

### 8.4.5 WPA, WPA2, WPA2-MIX

Click **WIRELESS > Wi-Fi > Security > Edit**. Select **WPA**, **WPA2** or **WPA2-MIX** from the **Security Mode** list.

**Figure 93** WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX

The following table describes the labels in this screen.

**Table 37** WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select <b>WPA</b> , <b>WPA2</b> or <b>WPA2-MIX</b> from the drop-down list.
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.  This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again.  Enter a time interval between 600 and 65535 seconds.
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in <b>WPA(2)-PSK</b> mode.

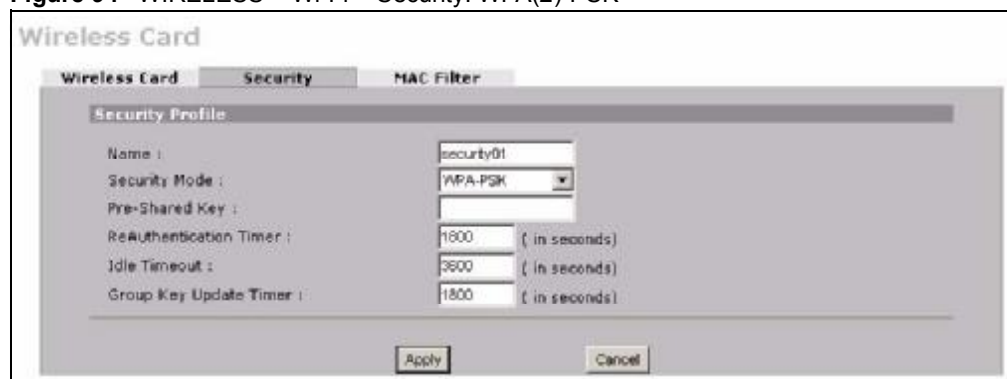


**Table 37** WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX (continued)

LABEL	DESCRIPTION
PMK Cache	This field is available only when you select <b>WPA2</b> or <b>WPA2-MIX</b> . When a wireless client moves from one AP's coverage area to another, it performs an authentication procedure (exchanging security information) with the new AP. Instead of re-authenticating a client each time it returns to the AP's coverage area, which can cause delays to time-sensitive applications, the AP and the client can store (or "cache") and use information about their previous authentication. Select <b>Enable</b> to allow PMK (Pairwise Master Key) caching, or <b>Disable</b> to switch this feature off.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

### 8.4.6 WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Click **WIRELESS > Wi-Fi > Security > Edit**. Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** from the **Security Mode** list.

**Figure 94** WIRELESS > Wi-Fi > Security: WPA(2)-PSK

The following table describes the labels in this screen.

**Table 38** WIRELESS > Wi-Fi > Security: WPA(2)-PSK

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select <b>WPA-PSK</b> , <b>WPA2-PSK</b> or <b>WPA2-PSK-MIX</b> from the drop-down list.
Pre-Shared Key	The encryption mechanisms used for <b>WPA(2)</b> and <b>WPA(2)-PSK</b> are the same. The only difference between the two is that <b>WPA(2)-PSK</b> uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

**Table 38** WIRELESS > Wi-Fi > Security: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
Idle Timeout	<p>The ZyXEL Device automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.</p> <p>This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again.</p> <p>Enter a time interval between 600 and 65535 seconds.</p>
Group Key Update Timer	<p>The <b>Group Key Update Timer</b> is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in <b>WPA(2)-PSK</b> mode.</p>
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 8.5 MAC Filter

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to specific devices (**Allow**) or exclude specific 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 addresses of the devices to configure this screen.

To change your ZyXEL Device's MAC filter settings, click the **WIRELESS > Wi-Fi > MAC Filter**. The screen appears as shown.



To activate MAC filtering on a profile, select **Enable** from the **Enable MAC Filtering** drop-down list box in the **Wireless Card > Edit** screen and click **Apply**.

**Figure 95** WIRELESS > Wi-Fi > MAC Filter

The screenshot shows the 'MAC Filter' configuration page. It features a table with 12 rows for adding MAC addresses. Each row has three columns: an index number (#), a text field for 'User Name', and a text field for 'MAC Address'. Above the table, there are radio buttons for 'Allow' (selected) and 'Deny'. At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this menu.

**Table 39** WIRELESS > Wi-Fi > MAC Filter

LABEL	DESCRIPTION
Association	Define the filter action for the list of MAC addresses in the MAC address filter table. Select <b>Deny</b> to block access to the router, MAC addresses not listed will be allowed to access the router. Select <b>Allow</b> to permit access to the router, MAC addresses not listed will be denied access to the router.
#	This is the index number of the MAC address.
User Name	Enter a descriptive name for the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless stations that are allowed or denied access to the ZyXEL Device in these address fields.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



---

# PART IV

## Security

---

Firewall (167)

Certificates (195)

Authentication Server (191)



# Firewall

This chapter shows you how to configure your ZyXEL Device's firewall.

## 9.1 Firewall Overview

The networking term firewall is a system or group of systems that enforces an access-control policy between two networks. It is generally a mechanism used to protect a trusted network from an untrusted network.

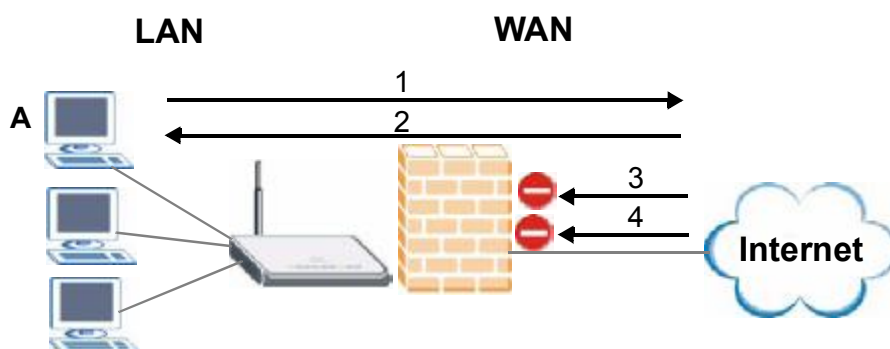
The ZyXEL Device physically separates the LAN, DMZ and the WAN and acts as a secure gateway for all data passing between the networks. The ZyXEL Device protects against Denial of Service (DoS) attacks, prevents theft, destruction and modification of data, and logs events.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN, DMZ and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.
- allows traffic that originates on the WAN to go to the DMZ and protects your DMZ computers against DoS attacks.

The following figure illustrates the default firewall action. User A can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

**Figure 96** Default Firewall Action



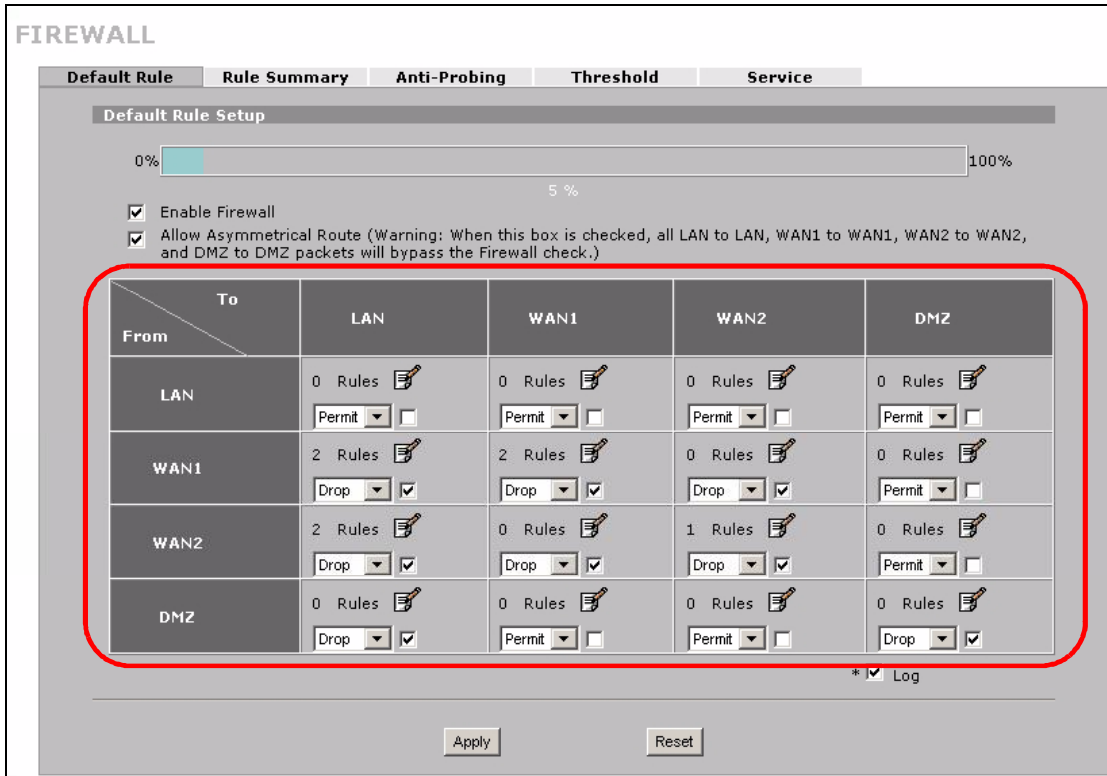
Your customized rules take precedence and override the ZyXEL Device's default settings. The ZyXEL Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyXEL Device takes the action specified in the rule.

## 9.2 Packet Direction Matrix

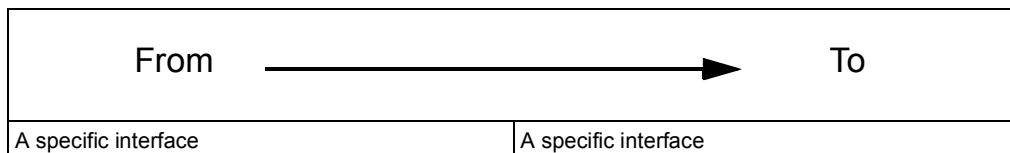
The ZyXEL Device’s packet direction matrix allows you to apply certain security settings (like firewall) to traffic flowing in specific directions.

For example, click **SECURITY > FIREWALL** to open the following screen. This screen configures general firewall settings.

**Figure 97** SECURITY > FIREWALL > Default Rule



Packets have a source and a destination. The packet direction matrix in the lower part of the screen sets what the ZyXEL Device does with packets traveling in a specific direction that do not match any of the firewall rules.



To set the ZyXEL Device to block traffic from WAN 1 from going to the DMZ interfaces, find where the **From WAN1** row and the **To DMZ** column intersect and set the field to **Drop** as shown.



Figure 98 Default Block Traffic From WAN1 to DMZ Example

**FIREWALL**

Default Rule   Rule Summary   Anti-Probing   Threshold   Service

**Default Rule Setup**

0%  100%

5%

Enable Firewall

Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN1 to WAN1, WAN2 to WAN2, and DMZ to DMZ packets will bypass the Firewall check.)

From \ To	LAN	WAN1	WAN2	DMZ
LAN	0 Rules Permit <input type="checkbox"/>	0 Rules Permit <input type="checkbox"/>	0 Rules Permit <input type="checkbox"/>	0 Rules Permit <input type="checkbox"/>
WAN1	2 Rules Drop <input checked="" type="checkbox"/>	2 Rules Drop <input checked="" type="checkbox"/>	0 Rules Drop <input checked="" type="checkbox"/>	0 Rules Drop <input checked="" type="checkbox"/>
WAN2	2 Rules Drop <input checked="" type="checkbox"/>	0 Rules Drop <input checked="" type="checkbox"/>	1 Rules Drop <input checked="" type="checkbox"/>	0 Rules Permit <input type="checkbox"/>
DMZ	0 Rules Drop <input checked="" type="checkbox"/>	0 Rules Permit <input type="checkbox"/>	0 Rules Permit <input type="checkbox"/>	0 Rules Drop <input checked="" type="checkbox"/>

\*  Log

Apply   Reset

### 9.3 Packet Direction Examples

Firewall rules are grouped based on the direction of travel of packets to which they apply. This section gives some examples of why you might configure firewall rules for specific connection directions.

By default, the ZyXEL Device allows packets traveling in the following directions.:

- LAN to LAN These rules specify which computers on the LAN can manage the ZyXEL Device (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).



You can also configure the remote management settings to allow only a specific computer to manage the ZyXEL Device.

- LAN to WAN 1 These rules specify which computers on the LAN can access which computers or services connected to WAN 1. See [Section 9.5 on page 171](#) for an example.

By default, the ZyXEL Device drops packets traveling in the following directions.

- **WAN 1 to LAN** These rules specify which computers connected to WAN 1 can access which computers or services on the LAN. For example, you may create rules to:
  - Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
  - Allow public access to a Web server on your protected network. You could also block certain IP addresses from accessing it.



---

You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN. See [Section 12.5.3 on page 236](#) for an example.

---

- **WAN to WAN** By default the ZyXEL Device stops computers connected to WAN1 or WAN2 from managing the ZyXEL Device or using the ZyXEL Device as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the ZyXEL Device.



---

You also need to configure the remote management settings to allow a WAN computer to manage the ZyXEL Device.

---

## 9.4 Security Considerations



---

Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyXEL Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

---

Consider these security ramifications before creating a rule:

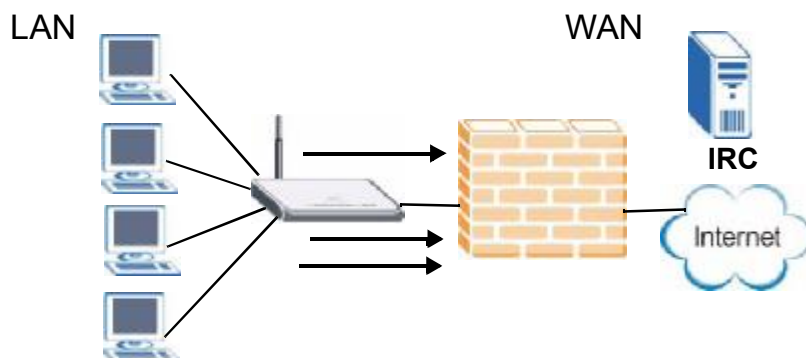
- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 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.
- 4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

## 9.5 Firewall Rules Example

Suppose that your company decides to block all of the LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

**Figure 99** Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

**Table 40** Blocking All LAN to WAN IRC Traffic Example

#	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	IRC	Drop
Default	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall's default policy that allows all traffic from the LAN to go to the WAN.

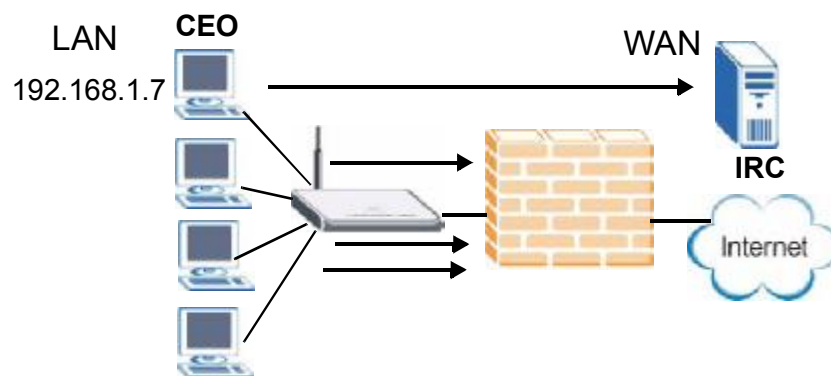
The ZyXEL Device applies the firewall rules in order. So for this example, when the ZyXEL Device receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the default rule and the ZyXEL Device forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

- has a static IP address,
- or you configure a static DHCP entry for it so the ZyXEL Device always assigns it the same IP address (see [Section 5.8 on page 106](#) for information on static DHCP).

Now you configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

**Figure 100** Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

**Table 41** Limited LAN to WAN IRC Traffic Example

#	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	192.168.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	IRC	Drop
Default	Any	Any	Any	Any	Allow

- The first row allows the LAN computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN access to the IRC service on the WAN.
- The third row is (still) the firewall's default policy of allowing all traffic from the LAN to go to the WAN.

The rule for the CEO must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ZyXEL Device would drop it and not check any other firewall rules.

## 9.6 Asymmetrical Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the ZyXEL Device's LAN IP address, return traffic may not go through the ZyXEL Device. This is called an asymmetrical or "triangle" route. This causes the ZyXEL Device to reset the connection, as the connection has not been acknowledged.

You can have the ZyXEL Device permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyXEL Device. A better solution is to use IP alias to put the ZyXEL Device and the backup gateway on separate subnets.

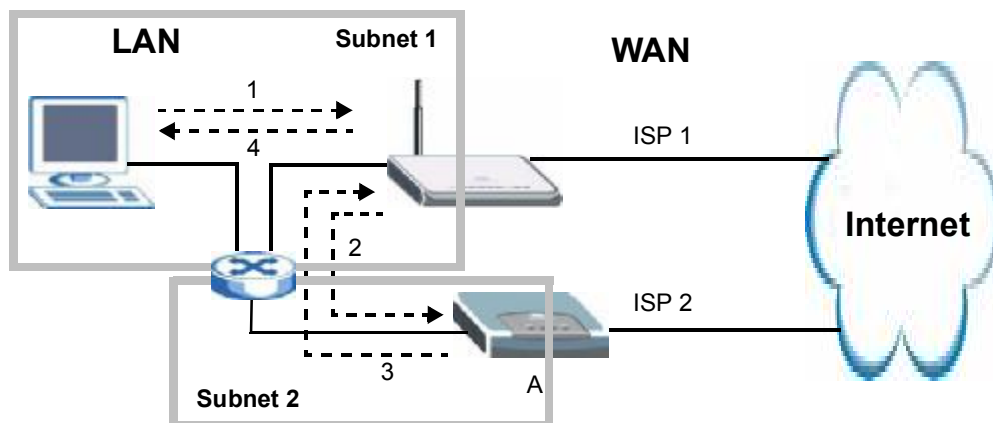
### 9.6.1 Asymmetrical Routes and IP Alias

You can use IP alias instead of allowing asymmetrical routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway A in different subnets, all returning network traffic must pass through the ZyXEL Device to your LAN. The following steps describe such a scenario.

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

**Figure 101** Using IP Alias to Solve the Triangle Route Problem

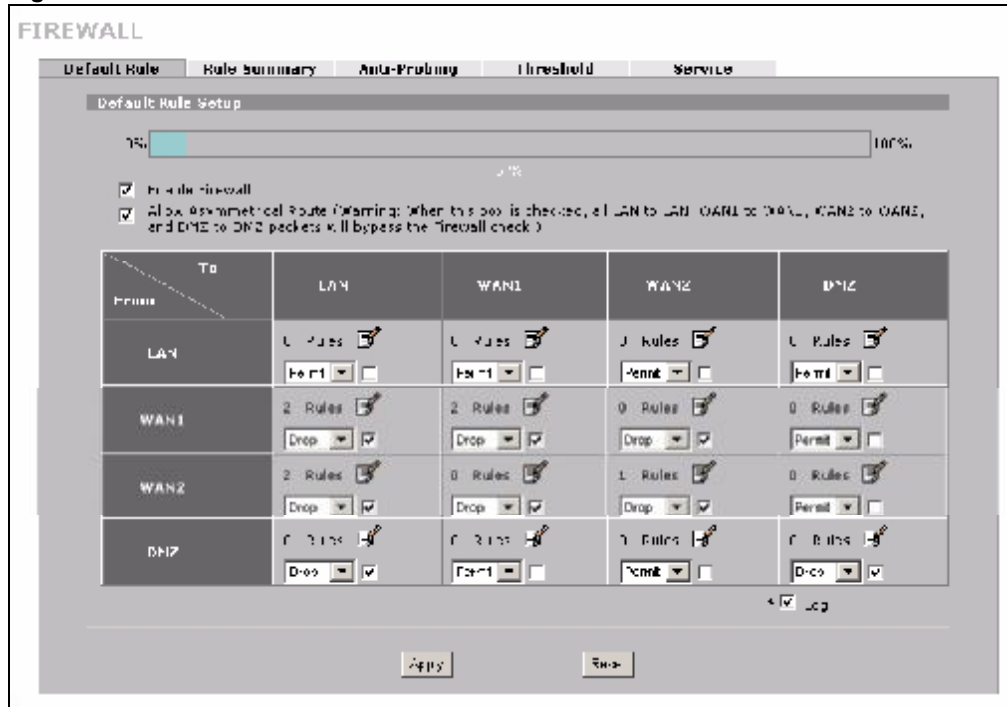


## 9.7 Firewall Default Rule

Click **SECURITY > FIREWALL** to open the **Default Rule** screen.

Use this screen to configure general firewall settings.

**Figure 102** SECURITY > FIREWALL > Default Rule



The following table describes the labels in this screen.

**Table 42** SECURITY > FIREWALL > Default Rule

LABEL	DESCRIPTION
0-100%	This bar displays the percentage of the ZyXEL Device's firewall rules storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary firewall rules before adding more firewall rules.
Enable 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.  Note: When you activate the firewall, all current connections through the ZyXEL Device are dropped when you apply your changes.
Allow Asymmetrical Route	If an alternate gateway on the LAN has an IP address in the same subnet as the ZyXEL Device's LAN IP address, return traffic may not go through the ZyXEL Device. This is called an asymmetrical or "triangle" route. This causes the ZyXEL Device to reset the connection, as the connection has not been acknowledged. Select this check box to have the ZyXEL Device permit the use of asymmetrical route topology on the network (not reset the connection).  Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyXEL Device. A better solution is to use IP alias to put the ZyXEL Device and the backup gateway on separate subnets. See <a href="#">Section 9.6.1 on page 173</a> for an example.

**Table 42** SECURITY > FIREWALL > Default Rule (continued)

LABEL	DESCRIPTION
From, To	<p>The firewall rules are grouped by the direction of packet travel. This displays the number of rules for each packet direction. Click the edit icon to go to a summary screen of the rules for that packet direction.</p> <p>Here is an example description of the directions of travel.</p> <p><b>From LAN To LAN</b> means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyXEL Device or the ZyXEL Device itself. The ZyXEL Device does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet.</p> <p>Use the drop-down list box to set the firewall's default actions based on the direction of travel of packets.</p> <p>Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select <b>Permit</b> to allow the passage of the packets.</p>
Log	<p>Select the check box next to a direction of packet travel to create a log when the above action is taken for packets that are traveling in that direction and do not match any of your customized rules.</p>
Apply	<p>Click <b>Apply</b> to save your changes.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 9.8 Firewall Rule Summary

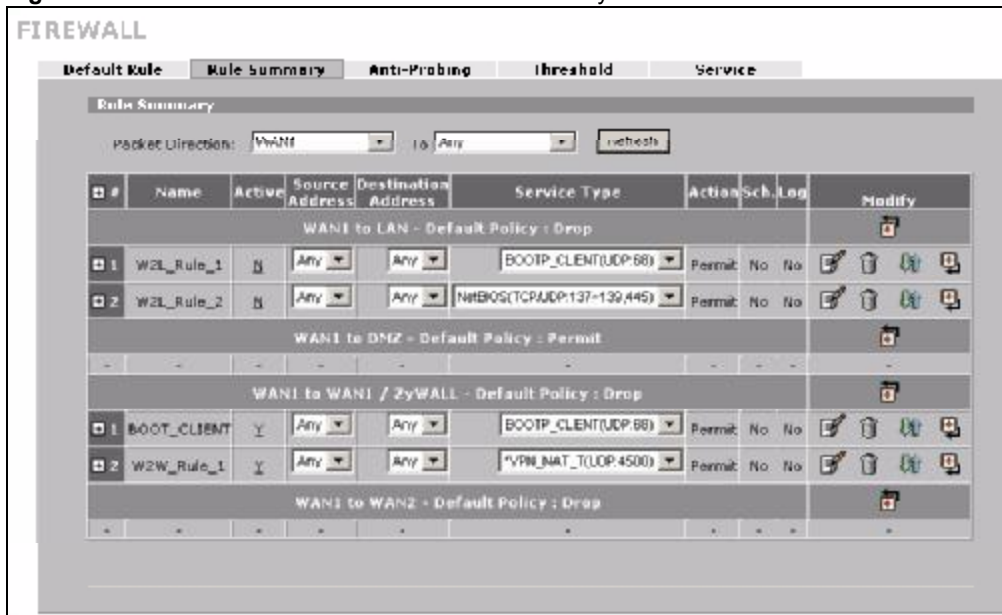
Click **SECURITY > FIREWALL > Rule Summary** to open the screen. This screen displays a list of the configured firewall rules.



The ordering of your rules is very important as rules are applied in the order that they are listed.

See [Section 9.1 on page 167](#) for more information about the firewall.

**Figure 103** SECURITY > FIREWALL > Rule Summary



The following table describes the labels in this screen.

**Table 43** SECURITY > FIREWALL > Rule Summary

LABEL	DESCRIPTION
Packet Direction	Use the drop-down list boxes and click <b>Refresh</b> to select a direction of travel of packets for which you want to display firewall rules.
+/-	In the heading row, click + to expand or - to collapse the <b>Source Address</b> , <b>Destination Address</b> and <b>Service Type</b> drop down lists for all of the displayed rules.
Default Policy	This field displays the default action you selected in the <b>Default Rule</b> screen for the packet direction displayed.
The following 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 above.	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click + to expand or - to collapse the <b>Source Address</b> , <b>Destination Address</b> and <b>Service Type</b> drop down lists.
Name	This is the name of the firewall rule.
Active	This field displays whether a firewall is turned on (Y) or not (N). Click the setting to change it.
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Service Type	This drop-down list box displays the services to which this firewall rule applies. Custom services have an * before the name. See <a href="#">Appendix D on page 385</a> for a list of common services.



**Table 43** SECURITY > FIREWALL > Rule Summary

LABEL	DESCRIPTION
Action	This field displays whether the firewall silently discards packets ( <b>Drop</b> ), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender ( <b>Reject</b> ) or allows the passage of packets ( <b>Permit</b> ).
Sch.	This field tells you whether a schedule is specified ( <b>Yes</b> ) or not ( <b>No</b> ).
Log	This field shows you whether a log is created when packets match this rule ( <b>Yes</b> ) or not ( <b>No</b> ).
Modify	<p>Click the edit icon to go to the screen where you can edit the rule.</p> <p>Click the delete 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.</p> <p>Click the insert icon to display the screen where you can configure a new firewall rule. The insert icon at the top of the row creates the new firewall rule before the others. The individual firewall rule insert icons create a new firewall rule after the row's firewall rule.</p> <p>Click the move icon, type an index number, and press Enter 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.</p>

### 9.8.1 Firewall Edit Rule

In the **Rule Summary** screen, click the edit icon or the insert icon to display the **Firewall Edit Rule** screen.

Use this screen to create or edit a firewall rule. Refer to the following table for information on the labels.

See [Section 9.1 on page 167](#) for more information about the firewall.

Figure 104 SECURITY > FIREWALL > Rule Summary > Edit

**FIREWALL - EDIT RULE**

Rule Name:

---

**Edit Source Address**

Address Editor

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

Source Address(es):

---

**Edit Destination Address**

Address Editor

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

Destination Address(es):

---

**Edit Service**

Available Services: (See [Service](#))

- ECHO\_REPLY(ICMP:Type:0&Code:0)
- ECHO\_REQUEST(ICMP:Type:8&Code:0)
- VPN\_NAT\_(UDP:4500)
- Any(All)
- Any(TCP)
- Any(UDP)
- Any(ICMP)
- AMANBY\_300(TCP:8180)
- AUTH(TCP:113)
- BORN(TCP:179)
- BOOTP\_CLIENT(UDP:68)
- BOOTP\_SERVER(UDP:67)
- CUI-SEENB(TCP:UDP:7648,24032)
- DNS(TCP:UDP:53)
- FINGER(TCP:79)

Selected Service(s):

---

**Edit Schedule**

Day to Apply:

Sun  Mon  Tue  Wed  Thu  Fri  Sat

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

All day

Start:  (Hour)  (Minute)    End:  (Hour)  (Minute)

---

**Actions When Matched**

Log Packet Information When Matched

Send Alert Message to Administrator When Matched

Action for Matched Packets:

The following table describes the labels in this screen.

**Table 44** SECURITY > FIREWALL > Rule Summary > Edit

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the firewall rule. Spaces are allowed.
Edit Source/ Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: <b>Single Address, Range Address, Subnet Address</b> and <b>Any Address</b> .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add	Click <b>Add</b> to add a new address to the <b>Source</b> or <b>Destination Address(es)</b> box. You can add multiple addresses, ranges of addresses, and/or subnets.
Modify	To edit an existing source or destination address, select it from the box and click <b>Modify</b> .
Delete	Highlight an existing source or destination address from the <b>Source</b> or <b>Destination Address(es)</b> box above and click <b>Delete</b> to remove it.
Edit Service	
Available/ Selected Services	Highlight a service from the <b>Available Services</b> box on the left, then click >> to add it to the <b>Selected Service(s)</b> box on the right. To remove a service, highlight it in the <b>Selected Service(s)</b> box on the right, then click <<. Next to the name of a 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 entry, (UDP/TCP:53) means UDP port 53 and TCP port 53. Click the <b>Service</b> link to go to the <b>Service</b> screen where you can configure custom service ports. See <a href="#">Appendix D on page 385</a> for a list of commonly used services and port numbers. You can use the [CTRL] key and select multiple services at once.
Edit Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select <b>All Day</b> or enter the start and end times in the hour-minute format to apply the rule.
Actions When Matched	
Log Packet Information When Matched	This field determines if a log for packets that match the rule is created ( <b>Yes</b> ) or not ( <b>No</b> ). Go to the <b>Log Settings</b> page and select the <b>Access Control</b> logs category to have the ZyXEL Device record these logs.
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 44** SECURITY > FIREWALL > Rule Summary > Edit

LABEL	DESCRIPTION
Action for Matched Packets	<p>Use the drop-down list box to select what the firewall is to do with packets that match this rule.</p> <p>Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.</p> <p>Select <b>Permit</b> to allow the passage of the packets.</p> <p>Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) if you want to allow computers on the WAN to access devices on the LAN.</p> <p>Note: You may also need to configure the remote management settings if you want to allow a WAN computer to manage the ZyXEL Device or restrict management from the LAN.</p>
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 9.9 Anti-Probing

Click **SECURITY > FIREWALL > Anti-Probing** to open the following screen. Configure this screen to help keep the ZyXEL Device hidden from probing attempts. You can specify which of the ZyXEL Device's interfaces will respond to Ping requests and whether or not the ZyXEL Device is to respond to probing for unused ports.

**Figure 105** SECURITY > FIREWALL > Anti-Probing

The screenshot shows the 'FIREWALL' configuration page with the 'Anti-Probing' tab selected. The 'Anti-Probing Setup' section contains the following options:

- Respond to PING on:
  - LAN
  - WAN1
  - WAN2
  - DMZ
- Do not respond to requests for unauthorized services.

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

The following table describes the labels in this screen.

**Table 45** SECURITY > FIREWALL > Anti-Probing

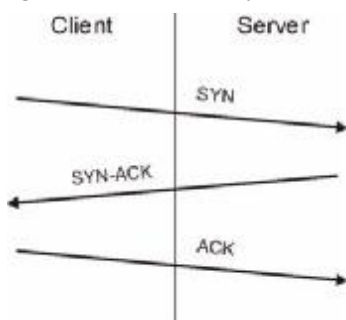
LABEL	DESCRIPTION
Respond to PING on	Select the check boxes of the interfaces that you want to reply to incoming Ping requests. Clear an interface's check box to have the ZyXEL Device not respond to any Ping requests that come into that interface.
Do not respond to requests for unauthorized services.	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. If this option is not selected, 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 rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyXEL Device reacts based on the firewall rule to either 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 <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 9.10 Firewall Thresholds

For DoS attacks, the ZyXEL Device uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. 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.

**Figure 106** Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

### 9.10.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the ZyXEL Device has been receiving DoS attacks that are not recorded in the logs or the logs show that the ZyXEL Device is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

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

Reduce the threshold values 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).

If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the ZyXEL Device may classify them as DoS attacks.

## 9.11 Threshold Screen

Click **SECURITY > FIREWALL > Threshold** to bring up the next screen. The global values specified for the threshold and timeout apply to all TCP connections.

**Figure 107** SECURITY > FIREWALL > Threshold

The screenshot shows the 'FIREWALL' configuration page with the 'Threshold' tab selected. At the top, there are tabs for 'Default Rule', 'Rule Summary', 'Anti-Probing', 'Threshold', and 'Service'. Below these, there are checkboxes to 'Disable DoS Attack Protection on' LAN, WAN1, WAN2, and DMZ. The main section is titled 'Denial of Service Thresholds' and contains the following settings:

Setting	Value	Unit
One Minute Low	80	sessions per minute
One Minute High	100	sessions per minute
Maximum Incomplete Low	80	sessions
Maximum Incomplete High	100	sessions
TCP Maximum Incomplete	30	sessions

Below this table, there is a section titled 'Action taken when TCP Maximum Incomplete reached threshold' with two radio button options:

- Delete the oldest half open session when new connection request comes.
- Deny new connection request for  (1~255 minutes)

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

The following table describes the labels in this screen.

**Table 46** SECURITY > FIREWALL > Threshold

LABEL	DESCRIPTION
Disable DoS Attack Protection on	Select the check boxes of any interfaces for which you want the ZyXEL Device to not use the Denial of Service protection thresholds. This disables DoS protection on the selected interface.  You may want to disable DoS protection for an interface if the ZyXEL Device is treating valid traffic as DoS attacks. Another option would be to raise the thresholds.
Denial of Service Thresholds	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.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	This is the rate of new half-open sessions per minute 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.  For example, if you set the one minute high to 100, the ZyXEL Device starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set <b>Maximum Incomplete High</b> to lower than the current <b>Maximum Incomplete Low</b> number.  For example, if you set the maximum incomplete high to 100, the ZyXEL Device starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.
TCP Maximum Incomplete	An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.  Specify 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. The ZyXEL Device sends alerts whenever the <b>TCP Maximum Incomplete</b> is exceeded.
Action taken when TCP Maximum Incomplete reached threshold	Select the action that ZyXEL Device should take when the TCP maximum incomplete threshold is reached. You can have the ZyXEL Device either:  Delete the oldest half open session when a new connection request comes. or  Deny new connection requests for the number of minutes that you specify (between 1 and 256).
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 9.12 Service

Click **SECURITY > FIREWALL > Service** to open the screen as shown next. Use this screen to configure custom services for use in firewall rules or view the services that are predefined in the ZyXEL Device.

See [Section 9.1 on page 167](#) for more information about the firewall.

**Figure 108** SECURITY > FIREWALL > Service

**FIREWALL**

Default Rule | Rule Summary | Anti-Probing | Threshold | **Service**

Custom Service

#	Service Name	Protocol	Attribute*	Modify
1	ECHO REPLY	ICMP	0/0	
2	ECHO REQUEST	ICMP	8/0	
3	VPN_NAT_T	UDP	4800	

\*Attribute: Port Range for TCP/UDP, Type/Code for ICMP.

Predefined Service

#	Service Name	Protocol	Attribute
1	Any_All	ALL	*
2	Any_TCP	TCP	1~65535
3	Any_UDP	UDP	1~65535
4	Any_ICMP	ICMP	*
5	AIM/NEW_ICQ	TCP	5190
6	AUTH	TCP	113
7	BGP	TCP	179
8	BOOTP_CLIENT	UDP	68
9	BOOTP_SERVER	UDP	67
10	CU-SEEEME	TCP/UDP	7648, 24032
11	DNS	TCP/UDP	53
12	FINGER	TCP	79
13	FTP	TCP	20, 21
14	H.323	TCP	1720
15	HTTP	TCP	80
16	HTTPS	TCP	443
17	IAX/IAX2	UDP	4869
18	IPSEC	TCP/UDP	500
19	IPSEC	TCP/UDP	4500
20	IPSEC	TCP/UDP	4500
21	IPSEC	TCP/UDP	4500
22	IPSEC	TCP/UDP	4500
23	IPSEC	TCP/UDP	4500
24	IPSEC	TCP/UDP	4500
25	IPSEC	TCP/UDP	4500
26	IPSEC	TCP/UDP	4500
27	IPSEC	TCP/UDP	4500
28	IPSEC	TCP/UDP	4500
29	IPSEC	TCP/UDP	4500
30	IPSEC	TCP/UDP	4500
31	IPSEC	TCP/UDP	4500
32	IPSEC	TCP/UDP	4500
33	IPSEC	TCP/UDP	4500
34	IPSEC	TCP/UDP	4500
35	IPSEC	TCP/UDP	4500
36	SQL-NET	TCP	1821
37	SSDP	UDP	1900
38	SSH	TCP	22
39	STRMWORKS	UDP	1558
40	SYSLOG	UDP	514
41	SUBMISSION	TCP/UDP	587
42	TACACS	UDP	49
43	TELNET	TCP	23
44	TFTP	UDP	69
45	VOOLIVE	TCP	7000
46	VNC	TCP	5900
47	Vantage_CNM	UDP	1864, 1865



The following table describes the labels in this screen.

**Table 47** SECURITY > FIREWALL > Service

LABEL	DESCRIPTION
Custom Service	This table shows all configured custom services.
#	This is the index number of the custom service.
Service Name	This is the name of the service.
Protocol	This is the IP protocol type. If you selected <b>Custom</b> , this is the IP protocol value you entered.
Attribute	This is the IP port number or ICMP type and code that defines the service.
Modify	Click the edit icon to go to the screen where you can edit the service. Click the delete icon to remove an existing service. A window displays asking you to confirm that you want to delete the service. Note that subsequent services move up by one when you take this action.
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Predefined Service	This table shows all the services that are already configured for use in firewall rules. See <a href="#">Appendix D on page 385</a> for a list of common services.
#	This is the index number of the predefined service.
Service Name	This is the name of the service.
Protocol	This is the IP protocol type. There may be more than one IP protocol type.
Attribute	This is the IP port number or ICMP type and code that defines the service.

### 9.12.1 Firewall Edit Custom Service

Click **SECURITY > FIREWALL > Service > Add** to display the following screen. Use this screen to configure a custom service entry not is not predefined in the ZyXEL Device. See [Appendix D on page 385](#) the user's guide appendices for a list of commonly used services and port numbers.

See [Section 9.1 on page 167](#) for more information about the firewall.

**Figure 109** Firewall Edit Custom Service

The following table describes the labels in this screen.

**Table 48** SECURITY > FIREWALL > Service > Add

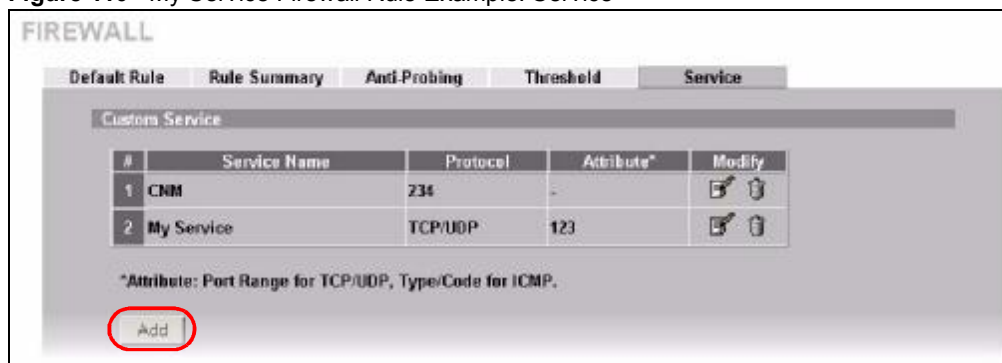
LABEL	DESCRIPTION
Service Name	Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the custom service. You cannot use the "(" character. Spaces are allowed.
IP Protocol	Choose the IP protocol ( <b>TCP</b> , <b>UDP</b> , <b>TCP/UDP</b> , <b>ICMP</b> or <b>Custom</b> ) that defines your customized service from the drop down list box. If you select <b>Custom</b> , specify the protocol's number. For example, ICMP is 1, TCP is 6, UDP is 17 and so on.
Port Range	Enter the port number (from 1 to 255) that defines the customized service To specify one port only, enter the port number in the <b>From</b> field and enter it again in the <b>To</b> field. To specify a span of ports, enter the first port in the <b>From</b> field and enter the last port in the <b>To</b> field.
Type/Code	This field is available only when you select <b>ICMP</b> in the <b>IP Protocol</b> field. The ICMP messages are identified by their types and in some cases codes. Enter the type number in the <b>Type</b> field and select the <b>Code</b> radio button and enter the code number if any.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 9.13 My Service Firewall Rule Example

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

- 1 In the **Service** screen, click **Add** to open the **Edit Custom Service** screen.

**Figure 110** My Service Firewall Rule Example: Service



- 2 Configure it as follows and click **Apply**.

**Figure 111** My Service Firewall Rule Example: Edit Custom Service

**FIREWALL - EDIT CUSTOM SERVICE**

Custom Service

Service Name: My Service

IP Protocol: TCP/UDP

Port Range: From 123 To 123

Apply (circled in red) Cancel

- 3 Click **Rule Summary**. Select **WAN1** and **LAN** from the **Packet Direction** drop-down list boxes and click **Refresh** to display existing firewall rules for the selected direction of travel of packets.
- 4 Click the insert icon at the top of the row to create the new firewall rule before the others.

**Figure 112** My Service Firewall Rule Example: Rule Summary

**FIREWALL**

Default Rule **Rule Summary** Anti-Probing Threshold Service

Rule Summary

Packet Direction: WAN1 To LAN Refresh (circled in red)

#	Name	Active	Source Address	Destination Address	Service Type	Action	Sch.	Log	Modify
WAN1 to LAN - Default Policy : Drop									
1	W2L_Rule_1	N	Any	Any	BOOTP_CLIENT(LDP:68)	Permit	No	No	(Edit, Delete, Refresh, Add icons)
2	W2L_Rule_2	N	Any	Any	NetBIOS(TCP/UDP:137-139,445)	Permit	No	No	(Edit, Delete, Refresh, Add icons)

The 'Modify' column header and the first icon in the first row of the table are circled in red.

- 5 The **Edit Rule** screen displays. Enter the name of the firewall rule.
- 6 Select **Any** in the **Destination Address(es)** box and then click **Delete**.
- 7 Configure the destination address fields as follows and click **Add**.

**Figure 113** My Service Firewall Rule Example: Rule Edit: Source and Destination Addresses

**FIREWALL - EDIT RULE**

Rule Name:

**Edit Source Address**

Address Editor

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

Source Address(es):

**Edit Destination Address**

Address Editor

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

Destination Address(es):

**Edit Service**

- 8 In the **Edit Service** section, use the arrows between **Available Services** and **Selected Service(s)** to configure it as follows. Click **Apply** when you are done.



Custom services show up with an \* before their names in the **Services** list boxes and the **Rule Summary** screen's **Service Type** list box.

Figure 114 My Service Firewall Rule Example: Edit Rule: Service Configuration

**FIREWALL - EDIT RULE**

Rule Name:

---

**Edit Source Address**

Address Editor

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

Source Address(es):

---

**Edit Destination Address**

Address Editor

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

Destination Address(es):

---

**Edit Service**

Available Services: (See [Service](#))

- \*ECHO-REPLY(ICMP.Type:0/Code:0)
- \*ECHO-REQUEST(ICMP.Type:8/Code:0)
- \*VPN\_NAT\_T(UDP:4500)
- Any(All)
- Any(TCP)
- Any(UDP)
- Any(ICMP)
- AMINEV\_IDG(TCP:5190)
- AUTH(TCP:113)
- BGP(TCP:179)
- BOOTP\_CLIENT(UDP:68)
- BOOTP\_SERVER(UDP:67)
- CL-SERNE(TCP/UDP:7648,24032)
- DNS(TCP/UDP:53)
- FINGER(TCP:79)

Selected Service(s):

---

**Edit Schedule**

Day to Apply:

Sun  Mon  Tue  Wed  Thu  Fri  Sat

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

All day

Start:  (Hour)  (Minute)    End:  (Hour)  (Minute)

---

**Actions When Matched**

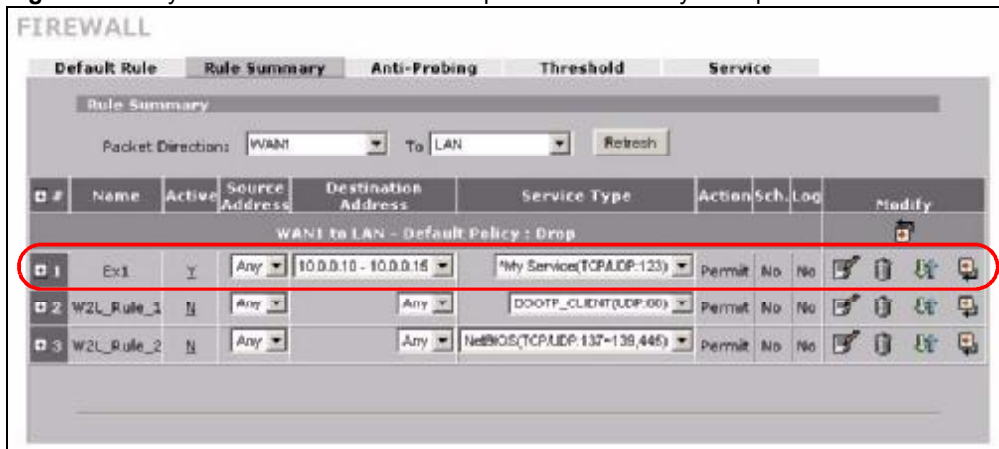
Log Packet Information When Matched

Send Alert Message to Administrator When Matched

Action for Matched Packets:

Rule 1 allows a My Service connection from WAN 1 to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

Figure 115 My Service Firewall Rule Example: Rule Summary: Completed



# Authentication Server

This chapter discusses how to configure the ZyXEL Device's authentication server feature.

## 10.1 Authentication Server Overview

A ZyXEL Device can use either the local user database internal to the ZyXEL Device or an external RADIUS server to authenticate wireless clients. See [Appendix E on page 389](#) for more information about RADIUS.

## 10.2 Local User Database

Click **SECURITY > AUTH SERVER** to open the **Local User Database** screen. The local user database is a list of user profiles stored on the ZyXEL Device. The ZyXEL Device can use this list of user profiles to authenticate users. Use this screen to change your ZyXEL Device's list of user profiles.

Figure 116 SECURITY > AUTH SERVER > Local User Database

AUTHENTICATION SERVER

Local User Database      RADIUS

User Database

#	Active	User Name	Password
1	<input type="checkbox"/>		
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		
11	<input type="checkbox"/>		
12	<input type="checkbox"/>		
13	<input type="checkbox"/>		
14	<input type="checkbox"/>		
15	<input type="checkbox"/>		
16	<input type="checkbox"/>		
17	<input type="checkbox"/>		
18	<input type="checkbox"/>		
19	<input type="checkbox"/>		
20	<input type="checkbox"/>		
21	<input type="checkbox"/>		
22	<input type="checkbox"/>		
23	<input type="checkbox"/>		
24	<input type="checkbox"/>		
25	<input type="checkbox"/>		
26	<input type="checkbox"/>		
27	<input type="checkbox"/>		
28	<input type="checkbox"/>		
29	<input type="checkbox"/>		
30	<input type="checkbox"/>		
31	<input type="checkbox"/>		
32	<input type="checkbox"/>		

Apply      Reset



The following table describes the labels in this screen.

**Table 49** SECURITY > AUTH SERVER > Local User Database

LABEL	DESCRIPTION
Active	Select this check box to enable the user profile.
User Name	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 10.3 RADIUS

Click **SECURITY > AUTH SERVER > RADIUS** to open the **RADIUS** screen. Configure this screen to use an external RADIUS server to authenticate users.

**Figure 117** SECURITY > AUTH SERVER > RADIUS

The following table describes the labels in this screen.

**Table 50** SECURITY > AUTH SERVER > RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the ZyXEL Device.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.

**Table 50** SECURITY > AUTH SERVER > RADIUS

LABEL	DESCRIPTION
Key	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 is not sent over the network. This key must be the same on the external authentication server and ZyXEL Device.
Accounting Server	
Active	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Key	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 is not sent over the network. This key must be the same on the external accounting server and ZyXEL Device.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# Certificates

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

## 11.1 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.

When using public-key cryptology for authentication, 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-private 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. The method used to secure the data that you send through an established connection depends on the type of connection.

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).

### 11.1.1 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.

## 11.2 Self-signed Certificates

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

## 11.3 Verifying a Certificate

Before you import a trusted CA or trusted remote host certificate into the ZyXEL Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the ZyXEL Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

### 11.3.1 Checking the Fingerprint of a Certificate on Your Computer

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

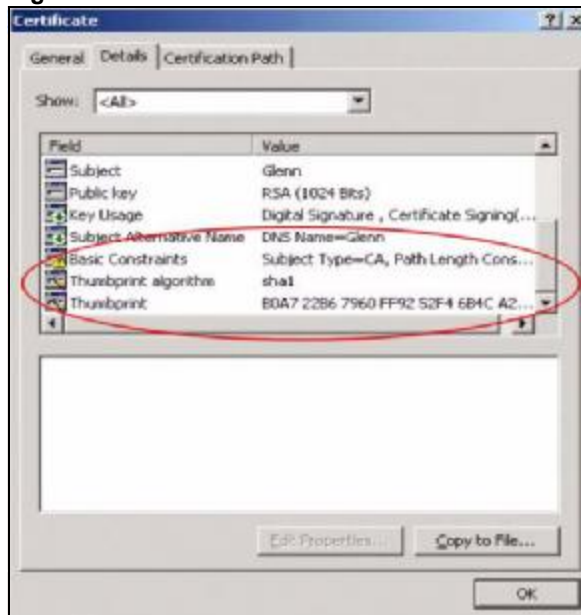
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 118** Certificates on Your Computer



- 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 119 Certificate Details

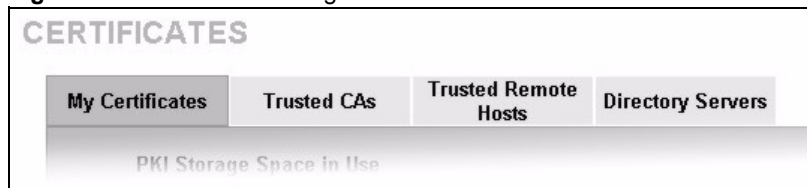


- 4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

## 11.4 Configuration Summary

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

Figure 120 Certificate Configuration Overview



Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.

Use the **Trusted CA** screens to save the certificates of trusted CAs to the ZyXEL Device. You can also export the certificates to a computer.

Use the **Trusted Remote Hosts** screens to import self-signed certificates from trusted remote hosts.

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

## 11.5 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 121** SECURITY > CERTIFICATES > My Certificates



The following table describes the labels in this screen.

**Table 51** SECURITY > CERTIFICATES > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. When the storage space is almost full, 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.
Type	This field displays what kind of certificate this is. <b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request. <b>SELF</b> represents a self-signed certificate. <b>*SELF</b> represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates. <b>CERT</b> represents a certificate issued by a certification authority.

**Table 51** SECURITY > CERTIFICATES > My Certificates (continued)

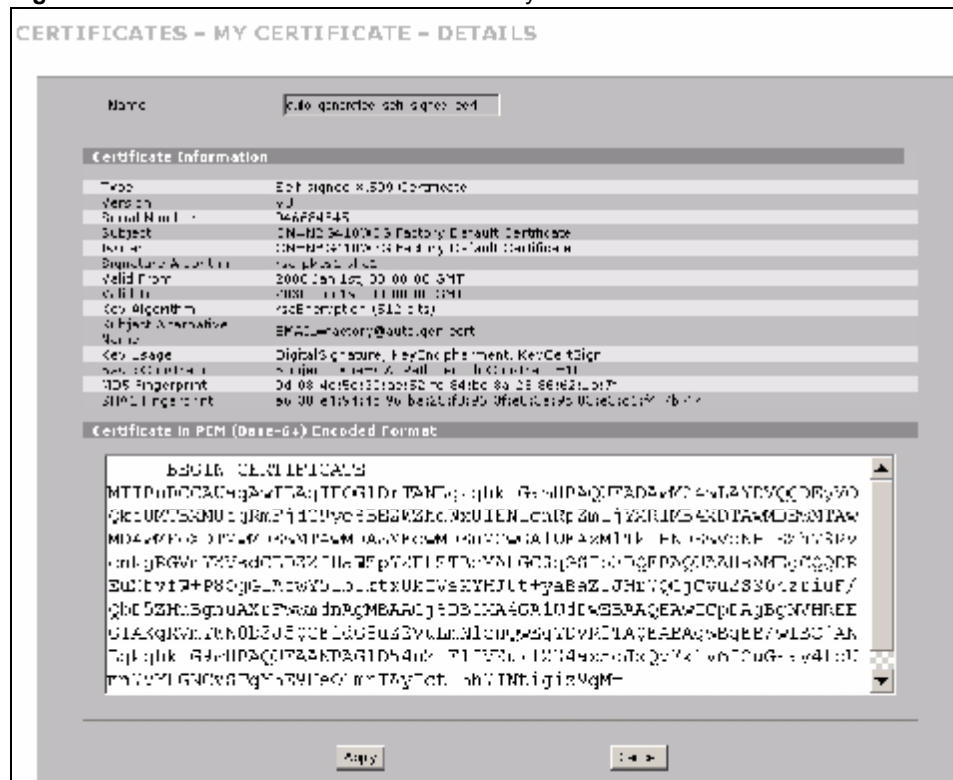
LABEL	DESCRIPTION
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	<p>Click the details icon to open a screen with an in-depth list of information about the certificate (or certification request).</p> <p>Click the export icon to save the certificate to a computer. For a certification request, click the export icon and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b>.</p> <p>Click the delete icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows <b>*SELF</b> in the <b>Type</b> field.</p> <ol style="list-style-type: none"> <li>1. Make sure that no other features, such as HTTPS, SSH are configured to use the <b>*SELF</b> certificate.</li> <li>2. Click the details icon next to another self-signed certificate (see the description on the <b>Create</b> button if you need to create a self-signed certificate).</li> <li>3. Select the <b>Default self-signed certificate which signs the imported remote host certificates</b> check box.</li> <li>4. Click <b>Apply</b> to save the changes and return to the <b>My Certificates</b> screen.</li> <li>5. The certificate that originally showed <b>*SELF</b> displays <b>SELF</b> and you can delete it now.</li> </ol> <p>Note that subsequent certificates move up by one when you take this action. The poll now icon displays when the ZyXEL Device generates a certification request successfully but the CA does not issue a certificate and sends a pending notification to the ZyXEL Device. If the icon displays, you can manually click the icon to have the ZyXEL Device query the CA (or RA (Registration Authority)) server for a certificate immediately. Otherwise, the ZyXEL Device checks with the server and updates the status periodically. The poll now icon disappears after the ZyWALL gets a certificate or the request has failed permanently due to being rejected by the CA server.</p>
Import	Click <b>Import</b> to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.
Create	Click <b>Create</b> to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.
Refresh	Click <b>Refresh</b> to display the current validity status of the certificates.

## 11.6 My Certificate Details

Click **SECURITY > CERTIFICATES > My Certificates** to open the **My Certificates** screen (see [Figure 121 on page 198](#)). 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.

If it is a self-signed certificate, you can also set the ZyXEL Device to use the certificate to sign the imported trusted remote host certificates.

**Figure 122** SECURITY > CERTIFICATES > My Certificates > Details



The following table describes the labels in this screen.

**Table 52** SECURITY > CERTIFICATES > My Certificates > 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).
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.