

P-660HW-Dx v2

802.11g Wireless ADSL2+ 4-port Gateway

User's Guide

Version 3.40

3/2007

Edition 2



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.



It is recommended you use the web configurator to configure the ZyXEL Device.

- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Web Site
- Please refer to 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

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 P-660HW-D may be referred to as the “ZyXEL Device”, the “device” or the “system” 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 

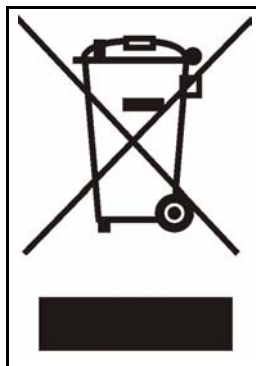
Safety Warnings



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 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.
- Please use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- 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

Introduction	31
Introducing the ZyXEL Device	33
Introducing the Web Configurator	39
Wizards	51
Wizard Setup for Internet Access	53
Bandwidth Management Wizard	67
Network	73
WAN Setup	75
LAN Setup	93
Wireless LAN	105
Network Address Translation (NAT) Screens	129
Security	141
Firewalls	143
Firewall Configuration	155
Content Filtering	177
Advanced	181
Static Route	183
Bandwidth Management	187
Dynamic DNS Setup	199
Remote Management Configuration	203
Universal Plug-and-Play (UPnP)	213
Maintenance and Troubleshooting	225
System	227
Logs	233
Tools	251
Diagnostic	257
Troubleshooting	259
Appendices and Index	263

Table of Contents

About This User's Guide	3
Document Conventions.....	4
Safety Warnings.....	6
Contents Overview	9
Table of Contents.....	11
List of Figures	21
List of Tables.....	27
Part I: Introduction.....	31
Chapter 1	
Introducing the ZyXEL Device	33
1.1 Overview	33
1.2 Ways to Manage the ZyXEL Device	35
1.3 Good Habits for Managing the ZyXEL Device	35
1.4 LEDs	35
1.5 Hardware Connections	36
1.5.1 Splitters and Microfilters	36
Chapter 2	
Introducing the Web Configurator	39
2.1 Web Configurator Overview	39
2.2 Accessing the Web Configurator	39
2.2.1 User Access	40
2.2.2 Administrator Access	40
2.3 Resetting the ZyXEL Device	42
2.3.1 Using the Reset Button	42
2.4 Navigating the Web Configurator	42
2.4.1 Navigation Panel	42
2.4.2 Status Screen	44
2.4.3 Status: Any IP Table	47
2.4.4 Status: WLAN Status	47
2.4.5 Status: Bandwidth Status	48

2.4.6 Status: Packet Statistics	48
2.4.7 Changing Login Password	50
Part II: Wizards	51
Chapter 3	
Wizard Setup for Internet Access.....	53
3.1 Introduction	53
3.2 Internet Access Wizard Setup	53
3.2.1 Automatic Detection	55
3.2.2 Manual Configuration	55
3.3 Wireless Connection Wizard Setup	60
3.3.1 Manually assign a WPA-PSK key	63
3.3.2 Manually assign a WEP key	63
Chapter 4	
Bandwidth Management Wizard.....	67
4.1 Introduction	67
4.2 Predefined Media Bandwidth Management Services	67
4.3 Bandwidth Management Wizard Setup	68
Part III: Network.....	73
Chapter 5	
WAN Setup.....	75
5.1 WAN Overview	75
5.1.1 Encapsulation	75
5.1.2 Multiplexing	76
5.1.3 Encapsulation and Multiplexing Scenarios	76
5.1.4 VPI and VCI	77
5.1.5 IP Address Assignment	77
5.1.6 Nailed-Up Connection (PPP)	77
5.1.7 NAT	78
5.2 Metric	78
5.3 Traffic Shaping	78
5.3.1 ATM Traffic Classes	79
5.4 Zero Configuration Internet Access	80
5.5 Internet Connection	80
5.5.1 Configuring Advanced Internet Connection Setup	82
5.6 Configuring More Connections	84

5.6.1 More Connections Edit	85
5.6.2 Configuring More Connections Advanced Setup	88
5.7 Traffic Redirect	89
5.8 Configuring WAN Backup	89
Chapter 6	
LAN Setup.....	93
6.1 LAN Overview	93
6.1.1 LANs, WANs and the ZyXEL Device	93
6.1.2 DHCP Setup	94
6.1.3 DNS Server Address	94
6.1.4 DNS Server Address Assignment	94
6.2 LAN TCP/IP	95
6.2.1 IP Address and Subnet Mask	95
6.2.2 RIP Setup	96
6.2.3 Multicast	96
6.2.4 Any IP	97
6.3 Configuring LAN IP	98
6.3.1 Configuring Advanced LAN Setup	99
6.4 DHCP Setup	100
6.5 LAN Client List	101
6.6 LAN IP Alias	102
Chapter 7	
Wireless LAN.....	105
7.1 Wireless Network Overview	105
7.2 Wireless Security Overview	106
7.2.1 SSID	106
7.2.2 MAC Address Filter	106
7.2.3 User Authentication	106
7.2.4 Encryption	107
7.2.5 One-Touch Intelligent Security Technology (OTIST)	108
7.3 General Wireless LAN Screen	108
7.3.1 No Security	109
7.3.2 WEP Encryption	110
7.3.3 WPA-PSK/WPA2-PSK	111
7.3.4 WPA/WPA2	113
7.3.5 Wireless LAN Advanced Setup	115
7.4 OTIST	117
7.4.1 Enabling OTIST	117
7.4.2 Starting OTIST	119
7.4.3 Notes on OTIST	120
7.5 MAC Filter	121

7.6 WMM QoS	122
7.6.1 WMM QoS Example	122
7.6.2 WMM QoS Priorities	122
7.6.3 Services	123
7.7 QoS Screen	124
7.7.1 ToS (Type of Service) and WMM QoS	125
7.7.2 Application Priority Configuration	126
Chapter 8	
Network Address Translation (NAT) Screens.....	129
8.1 NAT Overview	129
8.1.1 NAT Definitions	129
8.1.2 What NAT Does	130
8.1.3 How NAT Works	130
8.1.4 NAT Application	130
8.1.5 NAT Mapping Types	131
8.2 SUA (Single User Account) Versus NAT	132
8.3 SIP ALG	132
8.4 NAT General Setup	133
8.5 Port Forwarding	133
8.5.1 Default Server IP Address	134
8.5.2 Port Forwarding: Services and Port Numbers	134
8.5.3 Configuring Servers Behind Port Forwarding (Example)	135
8.6 Configuring Port Forwarding	135
8.6.1 Port Forwarding Rule Edit	136
8.7 Address Mapping	137
8.7.1 Address Mapping Rule Edit	139
Part IV: Security	141
Chapter 9	
Firewalls.....	143
9.1 Firewall Overview	143
9.2 Types of Firewalls	143
9.2.1 Packet Filtering Firewalls	143
9.2.2 Application-level Firewalls	144
9.2.3 Stateful Inspection Firewalls	144
9.3 Introduction to ZyXEL's Firewall	144
9.3.1 Denial of Service Attacks	145
9.4 Denial of Service	145
9.4.1 Basics	145

9.4.2 Types of DoS Attacks	146
9.5 Stateful Inspection	148
9.5.1 Stateful Inspection Process	149
9.5.2 Stateful Inspection and the ZyXEL Device	150
9.5.3 TCP Security	150
9.5.4 UDP/ICMP Security	151
9.5.5 Upper Layer Protocols	151
9.6 Guidelines for Enhancing Security with Your Firewall	152
9.6.1 Security In General	152
9.7 Packet Filtering Vs Firewall	153
9.7.1 Packet Filtering:	153
9.7.2 Firewall	153
Chapter 10	
Firewall Configuration	155
10.1 Access Methods	155
10.2 Firewall Policies Overview	155
10.3 Rule Logic Overview	156
10.3.1 Rule Checklist	156
10.3.2 Security Ramifications	156
10.3.3 Key Fields For Configuring Rules	157
10.4 Connection Direction	157
10.4.1 LAN to WAN Rules	158
10.4.2 Alerts	158
10.5 General Firewall Policy	158
10.6 Firewall Rules Summary	159
10.6.1 Configuring Firewall Rules	161
10.6.2 Customized Services	164
10.6.3 Configuring a Customized Service	164
10.7 Example Firewall Rule	165
10.8 Predefined Services	169
10.9 Anti-Probing	171
10.10 DoS Thresholds	172
10.10.1 Threshold Values	172
10.10.2 Half-Open Sessions	173
10.10.3 Configuring Firewall Thresholds	173
Chapter 11	
Content Filtering	177
11.1 Content Filtering Overview	177
11.2 Configuring Keyword Blocking	177
11.3 Configuring the Schedule	178
11.4 Configuring Trusted Computers	179

Part V: Advanced	181
Chapter 12	
Static Route	183
12.1 Static Route	183
12.2 Configuring Static Route	183
12.2.1 Static Route Edit	184
Chapter 13	
Bandwidth Management.....	187
13.1 Bandwidth Management Overview	187
13.2 Application-based Bandwidth Management	187
13.3 Subnet-based Bandwidth Management	187
13.4 Application and Subnet-based Bandwidth Management	188
13.5 Scheduler	188
13.5.1 Priority-based Scheduler	188
13.5.2 Fairness-based Scheduler	189
13.6 Maximize Bandwidth Usage	189
13.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic	189
13.6.2 Maximize Bandwidth Usage Example	189
13.6.3 Bandwidth Management Priorities	191
13.7 Over Allotment of Bandwidth	191
13.8 Configuring Summary	191
13.9 Bandwidth Management Rule Setup	192
13.10 DiffServ	194
13.10.1 DSCP and Per-Hop Behavior	194
13.10.2 Rule Configuration	194
13.11 Bandwidth Monitor	197
Chapter 14	
Dynamic DNS Setup	199
14.1 Dynamic DNS Overview	199
14.1.1 DYNDNS Wildcard	199
14.2 Configuring Dynamic DNS	199
Chapter 15	
Remote Management Configuration	203
15.1 Remote Management Overview	203
15.1.1 Remote Management Limitations	204
15.1.2 Remote Management and NAT	204
15.1.3 System Timeout	204
15.2 WWW	204
15.3 Telnet	205

15.4 Configuring Telnet	205
15.5 Telnet Login	206
15.6 Configuring FTP	207
15.7 SNMP	207
15.7.1 Supported MIBs	209
15.7.2 SNMP Traps	209
15.7.3 Configuring SNMP	209
15.8 Configuring DNS	210
15.9 Configuring ICMP	211
Chapter 16	
Universal Plug-and-Play (UPnP).....	213
16.1 Introducing Universal Plug and Play	213
16.1.1 How do I know if I'm using UPnP?	213
16.1.2 NAT Traversal	213
16.1.3 Cautions with UPnP	213
16.2 UPnP and ZyXEL	214
16.2.1 Configuring UPnP	214
16.3 Installing UPnP in Windows Example	215
16.3.1 Installing UPnP in Windows Me	215
16.3.2 Installing UPnP in Windows XP	216
16.4 Using UPnP in Windows XP Example	217
16.4.1 Auto-discover Your UPnP-enabled Network Device	218
16.4.2 Web Configurator Easy Access	221
Part VI: Maintenance and Troubleshooting	225
Chapter 17	
System	227
17.1 General Setup	227
17.1.1 General Setup and System Name	227
17.1.2 General Setup	227
17.2 Time Setting	229
Chapter 18	
Logs	233
18.1 Logs Overview	233
18.1.1 Alerts and Logs	233
18.2 Viewing the Logs	233
18.3 Configuring Log Settings	234
18.3.1 Example E-mail Log	236

18.4 Log Descriptions	237
Chapter 19	
Tools.....	251
19.1 Firmware Upgrade	251
19.2 Configuration Screen	253
19.2.1 Backup Configuration	253
19.2.2 Restore Configuration	254
19.2.3 Back to Factory Defaults	255
19.3 Restart	255
Chapter 20	
Diagnostic	257
20.1 General Diagnostic	257
20.2 DSL Line Diagnostic	257
Chapter 21	
Troubleshooting.....	259
21.1 Power, Hardware Connections, and LEDs	259
21.2 ZyXEL Device Access and Login	260
21.3 Internet Access	261
Part VII: Appendices and Index	263
Appendix A Product Specifications and Wall Mounting.....	265
Appendix B Wireless LANs	271
Appendix C Setting up Your Computer's IP Address	285
Appendix D IP Addresses and Subnetting	301
Appendix E Firewall Commands	311
Appendix F Internal SPTGEN.....	317
Appendix G Pop-up Windows, JavaScripts and Java Permissions.....	333
Appendix H NetBIOS Filter Commands	339
Appendix I Triangle Route	341
Appendix J Legal Information.....	343
Appendix K Customer Support.....	347

Index..... 351

List of Figures

Figure 1 Protected Internet Access Applications	34
Figure 2 LAN-to-LAN Application Example	34
Figure 3 Front Panel	35
Figure 4 Connecting a POTS Splitter	37
Figure 5 Connecting a Microfilter	37
Figure 6 Connecting a Microfilter and Y-Connector	38
Figure 7 ZyXEL Device with ISDN	38
Figure 8 Password Screen	40
Figure 9 User status screen	40
Figure 10 Change Password at Login	41
Figure 11 Select a Mode	41
Figure 12 Web Configurator: Main Screen	42
Figure 13 Status Screen	45
Figure 14 Status: Any IP Table	47
Figure 15 Status: WLAN Status	47
Figure 16 Status: Bandwidth Status	48
Figure 17 Status: Packet Statistics	49
Figure 18 System General	50
Figure 19 Select a Mode	53
Figure 20 Wizard: Welcome	54
Figure 21 Auto Detection: No DSL Connection	54
Figure 22 Auto Detection: Failed	55
Figure 23 Auto-Detection: PPPoE	55
Figure 24 Internet Access Wizard Setup: ISP Parameters	56
Figure 25 Internet Connection with PPPoE	57
Figure 26 Internet Connection with RFC 1483	57
Figure 27 Internet Connection with ENET ENCAP	58
Figure 28 Internet Connection with PPPoA	59
Figure 29 Connection Test Failed-1	59
Figure 30 Connection Test Failed-2.	60
Figure 31 Connection Test Successful	60
Figure 32 Wireless LAN Setup Wizard 1	61
Figure 33 Wireless LAN Setup Wizard 2	62
Figure 34 Manually assign a WPA key	63
Figure 35 Manually assign a WEP key	64
Figure 36 Wireless LAN Setup 3	64
Figure 37 Internet Access and WLAN Wizard Setup Complete	65
Figure 38 Select a Mode	68

Figure 39 Wizard: Welcome	69
Figure 40 Bandwidth Management Wizard: General Information	69
Figure 41 Bandwidth Management Wizard: Configuration	70
Figure 42 Bandwidth Management Wizard: Complete	71
Figure 43 Example of Traffic Shaping	79
Figure 44 Internet Connection (PPPoE)	81
Figure 45 Advanced Internet Connection Setup	83
Figure 46 More Connections	84
Figure 47 More Connections Edit	86
Figure 48 More Connections Advanced Setup	88
Figure 49 Traffic Redirect Example	89
Figure 50 Traffic Redirect LAN Setup	89
Figure 51 WAN Backup Setup	90
Figure 52 LAN and WAN IP Addresses	93
Figure 53 Any IP Example	97
Figure 54 LAN IP	98
Figure 55 Advanced LAN Setup	99
Figure 56 DHCP Setup	100
Figure 57 LAN Client List	102
Figure 58 Physical Network & Partitioned Logical Networks	103
Figure 59 LAN IP Alias	103
Figure 60 Example of a Wireless Network	105
Figure 61 Wireless LAN: General	108
Figure 62 Wireless: No Security	110
Figure 63 Wireless: Static WEP Encryption	111
Figure 64 Wireless: WPA-PSK/WPA2-PSK	112
Figure 65 Wireless: WPA/WPA2	114
Figure 66 Advanced	116
Figure 67 OTIST	118
Figure 68 Example Wireless Client OTIST Screen	119
Figure 69 Security Key	119
Figure 70 OTIST in Progress (AP)	119
Figure 71 OTIST in progress (Client)	120
Figure 72 No AP with OTIST Found	120
Figure 73 Start OTIST?	120
Figure 74 MAC Address Filter	121
Figure 75 Wireless LAN: QoS	125
Figure 76 Application Priority Configuration	126
Figure 77 How NAT Works	130
Figure 78 NAT Application With IP Alias	131
Figure 79 NAT General	133
Figure 80 Multiple Servers Behind NAT Example	135
Figure 81 NAT Port Forwarding	136

Figure 82 Port Forwarding Rule Setup	137
Figure 83 Address Mapping Rules	138
Figure 84 Edit Address Mapping Rule	139
Figure 85 Firewall Application	145
Figure 86 Three-Way Handshake	146
Figure 87 SYN Flood	147
Figure 88 Smurf Attack	147
Figure 89 Stateful Inspection	149
Figure 90 Firewall: General	158
Figure 91 Firewall Rules	160
Figure 92 Firewall: Edit Rule	162
Figure 93 Firewall: Customized Services	164
Figure 94 Firewall: Configure Customized Services	165
Figure 95 Firewall Example: Rules	166
Figure 96 Edit Custom Port Example	166
Figure 97 Firewall Example: Edit Rule: Destination Address	167
Figure 98 Firewall Example: Edit Rule: Select Customized Services	168
Figure 99 Firewall Example: Rules: MyService	169
Figure 100 Firewall: Anti Probing	171
Figure 101 Firewall: Threshold	174
Figure 102 Content Filter: Keyword	177
Figure 103 Content Filter: Schedule	178
Figure 104 Content Filter: Trusted	179
Figure 105 Example of Static Routing Topology	183
Figure 106 Static Route	184
Figure 107 Static Route Edit	185
Figure 108 Subnet-based Bandwidth Management Example	188
Figure 109 Bandwidth Management: Summary	192
Figure 110 Bandwidth Management: Rule Setup	193
Figure 111 DiffServ: Differentiated Service Field	194
Figure 112 Bandwidth Management Rule Configuration	195
Figure 113 Bandwidth Management: Monitor	198
Figure 114 Dynamic DNS	200
Figure 115 Remote Management: WWW	204
Figure 116 Telnet Configuration on a TCP/IP Network	205
Figure 117 Remote Management: Telnet	206
Figure 118 Remote Management: FTP	207
Figure 119 SNMP Management Model	208
Figure 120 Remote Management: SNMP	209
Figure 121 Remote Management: DNS	211
Figure 122 Remote Management: ICMP	212
Figure 123 Configuring UPnP	214
Figure 124 Add/Remove Programs: Windows Setup: Communication	215

Figure 125 Add/Remove Programs: Windows Setup: Communication: Components	216
Figure 126 Network Connections	216
Figure 127 Windows Optional Networking Components Wizard	217
Figure 128 Networking Services	217
Figure 129 Network Connections	218
Figure 130 Internet Connection Properties	219
Figure 131 Internet Connection Properties: Advanced Settings	219
Figure 132 Internet Connection Properties: Advanced Settings: Add	220
Figure 133 System Tray Icon	220
Figure 134 Internet Connection Status	221
Figure 135 Network Connections	222
Figure 136 Network Connections: My Network Places	223
Figure 137 Network Connections: My Network Places: Properties: Example	223
Figure 138 System General Setup	228
Figure 139 System Time Setting	229
Figure 140 View Log	234
Figure 141 Log Settings	235
Figure 142 E-mail Log Example	237
Figure 143 Firmware	251
Figure 144 Firmware Upload In Progress	252
Figure 145 Network Temporarily Disconnected	252
Figure 146 Error Message	253
Figure 147 Configuration	253
Figure 148 Configuration Restore Successful	254
Figure 149 Temporarily Disconnected	254
Figure 150 Configuration Restore Error	255
Figure 151 Restart Screen	255
Figure 152 Diagnostic: General	257
Figure 153 Diagnostic: DSL Line	258
Figure 154 Wall-mounting Example	269
Figure 155 Masonry Plug and M4 Tap Screw	270
Figure 156 Peer-to-Peer Communication in an Ad-hoc Network	271
Figure 157 Basic Service Set	272
Figure 158 Infrastructure WLAN	273
Figure 159 RTS/CTS	274
Figure 160 WPA(2) with RADIUS Application Example	281
Figure 161 WPA(2)-PSK Authentication	282
Figure 162 WIndows 95/98/Me: Network: Configuration	286
Figure 163 Windows 95/98/Me: TCP/IP Properties: IP Address	287
Figure 164 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	288
Figure 165 Windows XP: Start Menu	289
Figure 166 Windows XP: Control Panel	289
Figure 167 Windows XP: Control Panel: Network Connections: Properties	290

Figure 168 Windows XP: Local Area Connection Properties	290
Figure 169 Windows XP: Internet Protocol (TCP/IP) Properties	291
Figure 170 Windows XP: Advanced TCP/IP Properties	292
Figure 171 Windows XP: Internet Protocol (TCP/IP) Properties	293
Figure 172 Macintosh OS 8/9: Apple Menu	294
Figure 173 Macintosh OS 8/9: TCP/IP	294
Figure 174 Macintosh OS X: Apple Menu	295
Figure 175 Macintosh OS X: Network	296
Figure 176 Red Hat 9.0: KDE: Network Configuration: Devices	297
Figure 177 Red Hat 9.0: KDE: Ethernet Device: General	297
Figure 178 Red Hat 9.0: KDE: Network Configuration: DNS	298
Figure 179 Red Hat 9.0: KDE: Network Configuration: Activate	298
Figure 180 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	299
Figure 181 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	299
Figure 182 Red Hat 9.0: DNS Settings in resolv.conf	299
Figure 183 Red Hat 9.0: Restart Ethernet Card	299
Figure 184 Red Hat 9.0: Checking TCP/IP Properties	300
Figure 185 Network Number and Host ID	302
Figure 186 Subnetting Example: Before Subnetting	304
Figure 187 Subnetting Example: After Subnetting	305
Figure 188 Conflicting Computer IP Addresses Example	309
Figure 189 Conflicting Computer IP Addresses Example	309
Figure 190 Conflicting Computer and Router IP Addresses Example	310
Figure 191 Configuration Text File Format: Column Descriptions	317
Figure 192 Invalid Parameter Entered: Command Line Example	318
Figure 193 Valid Parameter Entered: Command Line Example	318
Figure 194 Internal SPTGEN FTP Download Example	319
Figure 195 Internal SPTGEN FTP Upload Example	319
Figure 196 Pop-up Blocker	333
Figure 197 Internet Options: Privacy	334
Figure 198 Internet Options: Privacy	335
Figure 199 Pop-up Blocker Settings	335
Figure 200 Internet Options: Security	336
Figure 201 Security Settings - Java Scripting	337
Figure 202 Security Settings - Java	337
Figure 203 Java (Sun)	338
Figure 204 Ideal Setup	341
Figure 205 "Triangle Route" Problem	342
Figure 206 IP Alias	342

List of Tables

Table 1 ADSL Standards	34
Table 2 Front Panel LEDs	36
Table 3 Web Configurator Screens Summary	43
Table 4 Status Screen	45
Table 5 Status: Any IP Table	47
Table 6 Status: WLAN Status	48
Table 7 Status: Packet Statistics	49
Table 8 Internet Access Wizard Setup: ISP Parameters	56
Table 9 Internet Connection with PPPoE	57
Table 10 Internet Connection with RFC 1483	57
Table 11 Internet Connection with ENET ENCAP	58
Table 12 Internet Connection with PPPoA	59
Table 13 Wireless LAN Setup Wizard 1	61
Table 14 Wireless LAN Setup Wizard 2	62
Table 15 Manually assign a WPA key	63
Table 16 Manually assign a WEP key	64
Table 17 Media Bandwidth Management Setup: Services	67
Table 18 Bandwidth Management Wizard: General Information	69
Table 19 Bandwidth Management Wizard: Configuration	70
Table 20 Internet Connection	81
Table 21 Advanced Internet Connection Setup	83
Table 22 More Connections	85
Table 23 More Connections Edit	86
Table 24 More Connections Advanced Setup	88
Table 25 WAN Backup Setup	90
Table 26 LAN IP	99
Table 27 Advanced LAN Setup	99
Table 28 DHCP Setup	101
Table 29 LAN Client List	102
Table 30 LAN IP Alias	104
Table 31 Types of Encryption for Each Type of Authentication	107
Table 32 Wireless LAN: General	109
Table 33 Wireless No Security	110
Table 34 Wireless: Static WEP Encryption	111
Table 35 Wireless: WPA-PSK/WPA2-PSK	112
Table 36 Wireless: WPA/WPA2	114
Table 37 Wireless LAN: Advanced	116
Table 38 OTIST	118

Table 39 MAC Address Filter	121
Table 40 WMM QoS Priorities	122
Table 41 Commonly Used Services	123
Table 42 Wireless Lan: QoS	125
Table 43 Application Priority Configuration	126
Table 44 NAT Definitions	129
Table 45 NAT Mapping Types	132
Table 46 NAT General	133
Table 47 Services and Port Numbers	134
Table 48 NAT Port Forwarding	136
Table 49 Port Forwarding Rule Setup	137
Table 50 Address Mapping Rules	138
Table 51 Edit Address Mapping Rule	140
Table 52 Common IP Ports	145
Table 53 ICMP Commands That Trigger Alerts	148
Table 54 Legal NetBIOS Commands	148
Table 55 Legal SMTP Commands	148
Table 56 Firewall: General	159
Table 57 Firewall Rules	160
Table 58 Firewall: Edit Rule	163
Table 59 Customized Services	164
Table 60 Firewall: Configure Customized Services	165
Table 61 Predefined Services	169
Table 62 Firewall: Anti Probing	172
Table 63 Firewall: Threshold	174
Table 64 Content Filter: Keyword	178
Table 65 Content Filter: Schedule	179
Table 66 Content Filter: Trusted	179
Table 67 Static Route	184
Table 68 Static Route Edit	185
Table 69 Application and Subnet-based Bandwidth Management Example	188
Table 70 Maximize Bandwidth Usage Example	189
Table 71 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example	190
Table 72 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example	190
Table 73 Bandwidth Management Priorities	191
Table 74 Over Allotment of Bandwidth Example	191
Table 75 Media Bandwidth Management: Summary	192
Table 76 Bandwidth Management: Rule Setup	193
Table 77 Sub-Classes of AF Services	194
Table 78 Bandwidth Management Rule Configuration	195
Table 79 Services and Port Numbers	197
Table 80 Bandwidth Management Monitor	198
Table 81 Dynamic DNS	200

Table 82 Remote Management: WWW	205
Table 83 Remote Management: Telnet	206
Table 84 Remote Management: FTP	207
Table 85 SNMP Traps	209
Table 86 Remote Management: SNMP	210
Table 87 Remote Management: DNS	211
Table 88 Remote Management: ICMP	212
Table 89 Configuring UPnP	214
Table 90 System General Setup	228
Table 91 System Time Setting	230
Table 92 View Log	234
Table 93 Log Settings	235
Table 94 System Maintenance Logs	237
Table 95 System Error Logs	238
Table 96 Access Control Logs	238
Table 97 TCP Reset Logs	239
Table 98 Packet Filter Logs	239
Table 99 ICMP Logs	240
Table 100 CDR Logs	240
Table 101 PPP Logs	240
Table 102 UPnP Logs	241
Table 103 Content Filtering Logs	241
Table 104 Attack Logs	242
Table 105 IPSec Logs	242
Table 106 IKE Logs	243
Table 107 PKI Logs	246
Table 108 Certificate Path Verification Failure Reason Codes	247
Table 109 ACL Setting Notes	247
Table 110 ICMP Notes	248
Table 111 Syslog Logs	249
Table 112 RFC-2408 ISAKMP Payload Types	249
Table 113 Firmware Upgrade	252
Table 114 Maintenance Restore Configuration	254
Table 115 Diagnostic: General	257
Table 116 Diagnostic: DSL Line	258
Table 117 Hardware Specifications	265
Table 118 Firmware Specifications	265
Table 119 Wireless Firmware Specifications	267
Table 120 Standards Supported	267
Table 121 IEEE 802.11g	275
Table 122 Wireless Security Levels	276
Table 123 Comparison of EAP Authentication Types	279
Table 124 Wireless Security Relational Matrix	282

Table 125 IP Address Network Number and Host ID Example	302
Table 126 Subnet Masks	303
Table 127 Maximum Host Numbers	303
Table 128 Alternative Subnet Mask Notation	303
Table 129 Subnet 1	305
Table 130 Subnet 2	306
Table 131 Subnet 3	306
Table 132 Subnet 4	306
Table 133 Eight Subnets	306
Table 134 24-bit Network Number Subnet Planning	307
Table 135 16-bit Network Number Subnet Planning	307
Table 136 Firewall Commands	311
Table 137 Abbreviations Used in the Example Internal SPTGEN Screens Table	320
Table 138 Menu 1 General Setup	320
Table 139 Menu 3	320
Table 140 Menu 4 Internet Access Setup	322
Table 141 Menu 12	324
Table 142 Menu 15 SUA Server Setup	324
Table 143 Menu 21.1 Filter Set #1	326
Table 144 Menu 21.1 Filter Set #2,	327
Table 145 Menu 23 System Menus	329
Table 146 Menu 24.11 Remote Management Control	330
Table 147 Command Examples	331
Table 148 NetBIOS Filter Default Settings	340

PART I

Introduction

Introducing the ZyXEL Device (33)

Introducing the Web Configurator (39)

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

The ZyXEL Device is an IEEE 802.11b/g wireless ADSL2+ gateway that allows super-fast, secure Internet access over analog (POTS), digital (ISDN) telephone lines (depending on your model) or by wireless.

In the ZyXEL Device product name, “H” denotes an integrated 4-port switch (hub) and “W” denotes an included wireless LAN card that provides wireless connectivity. D MEANS WHAT?

See the Product Specifications appendix for a full list of features.

Model names ending in “1”, for example P-660H/HW-D Series, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Model names ending in “3” denote a device that works over ISDN (Integrated Services Digital Network).

The DSL RJ-11 (ADSL over POTS models) or RJ-45 (ADSL over ISDN models) connects to your ADSL-enabled telephone line.



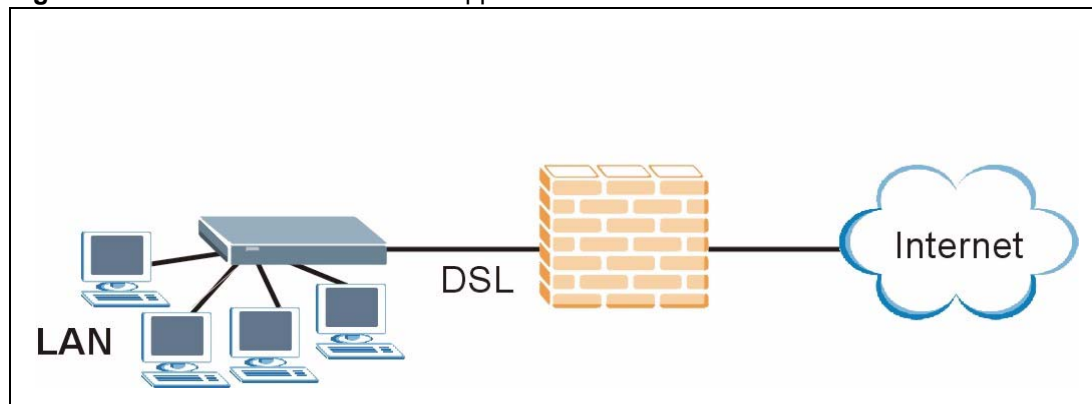
Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

The ZyXEL Device is the ideal high-speed Internet access solution. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers and supports the ADSL standards as shown in [Table 1 on page 34](#). In addition, the ZyXEL Device with its wireless features allows wireless clients access to your wired network resources and to the Internet.

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

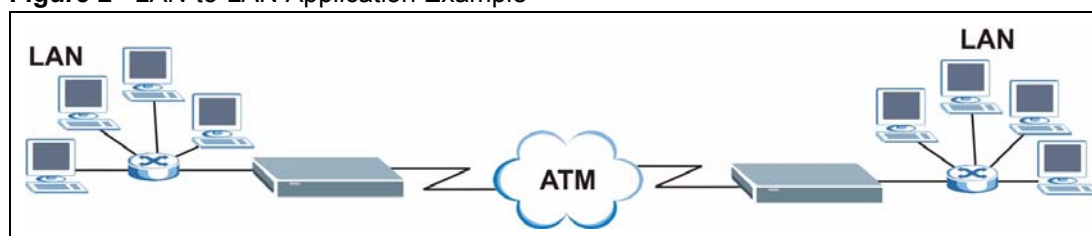
A typical Internet access application is shown below

Figure 1 Protected Internet Access Applications



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

Figure 2 LAN-to-LAN Application Example



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

Table 1 ADSL Standards

DATARATESTANDARD	UPSTREAM	DOWNSTREAM
ADSL	832 kbps	8Mbps
ADSL2	3.5Mbps	12Mbps
ADSL2+	3.5Mbps	24Mbps



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



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

1.2 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 ([Chapter 19 on page 251](#))
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- SPTGEN. SPTGEN is a text configuration file that allows you to configure the device by uploading an SPTGEN file. This is especially convenient if you need to configure many devices of the same type.

1.3 Good Habits for Managing the ZyXEL Device

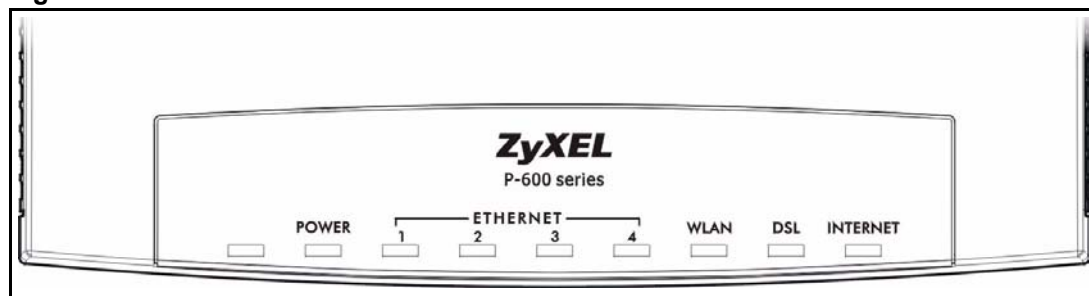
Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- 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.

1.4 LEDs

The following figure shows the ZyXEL Device's LEDs.

Figure 3 Front Panel



The following table describes the LEDs.

Table 2 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting or performing diagnostics.
	Red	On	Power to the ZyXEL Device is too low.
		Off	The system is not ready or has malfunctioned.
ETHERNET	Green	On	The ZyXEL Device has a successful 10Mb Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
	Amber	On	The ZyXEL Device has a successful 100Mb Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
		Off	The LAN is not connected.
WLAN	Green	On	The ZyXEL Device is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The ZyXEL Device is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
DSL	Green	On	The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The Internet connection is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.

1.5 Hardware Connections

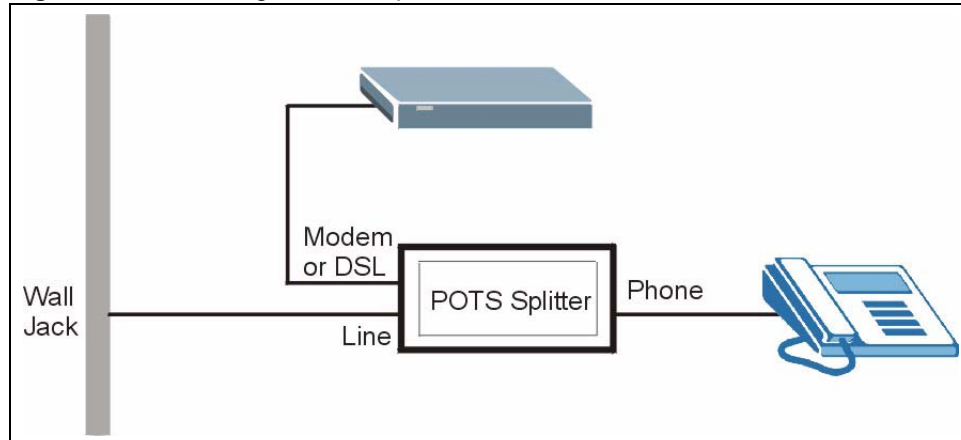
Refer to the Quick Start Guide for information on hardware connections.

1.5.1 Splitters and Microfilters

1.5.1.1 Connecting a POTS Splitter

When you use the Full Rate (G.dmt) ADSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitter at the point where the telephone line enters your residence, as shown in the following figure.

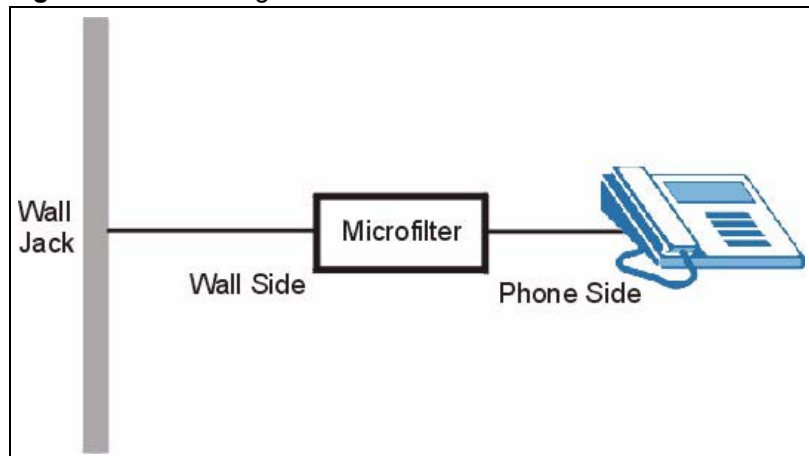
Figure 4 Connecting a POTS Splitter

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

1.5.1.2 Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.

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

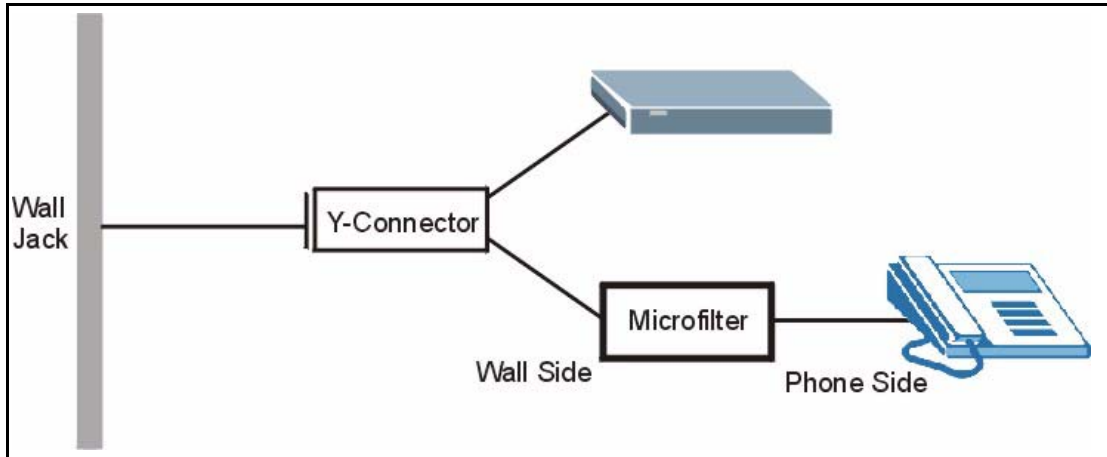
Figure 5 Connecting a Microfilter

You can also use a Y-Connector with a microfilter in order to connect both your modem and a telephone to the same wall jack without using a POTS splitter.

- 1 Connect a phone cable from the wall jack to the single jack end of the Y-Connector.

- 2 Connect a cable from the double jack end of the Y-Connector to the “wall side” of the microfilter.
- 3 Connect another cable from the double jack end of the Y-Connector to the ZyXEL Device.
- 4 Connect the “phone side” of the microfilter to your telephone as shown in the following figure.

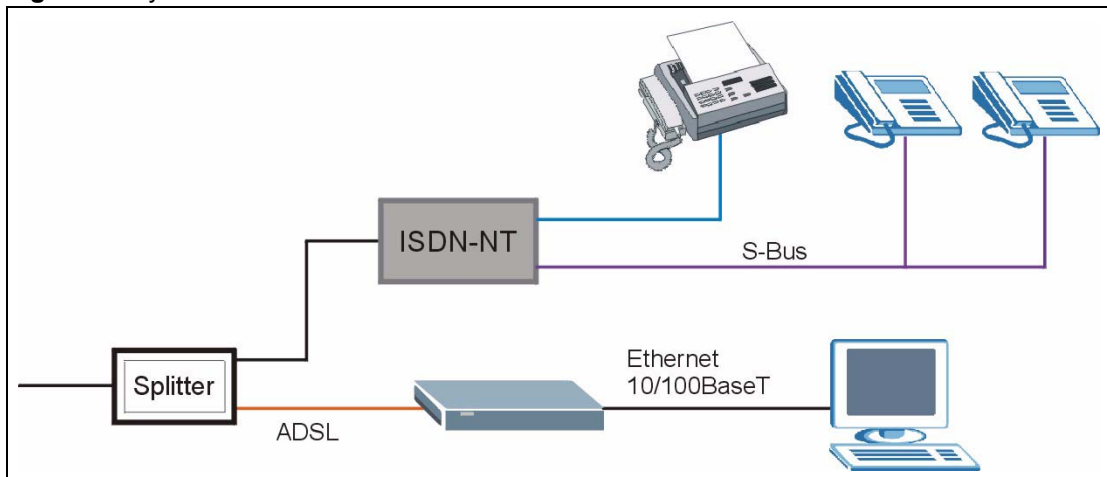
Figure 6 Connecting a Microfilter and Y-Connector



1.5.1.3 ZyXEL Device With ISDN

This section relates to people who use their ZyXEL Device with ADSL over ISDN (digital telephone service) only. The following is an example installation for the ZyXEL Device with ISDN.

Figure 7 ZyXEL Device with ISDN



Introducing the Web Configurator

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

2.1 Web Configurator Overview

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

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

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

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

2.2 Accessing the Web Configurator



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

- 1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Prepare your computer/computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
- 3 Launch your web browser.
- 4 Type "192.168.1.1" as the URL.

- 5 A window displays as shown.

Figure 8 Password Screen



2.2.1 User Access

- 1 For user access enter the default user password **user** to view the status only. The following window will appear.

Figure 9 User status screen

Interface	Status	Rate
DSL	Down	0 kbps / 0 kbps
LAN 1	Down	-
LAN 2	Down	-
LAN 3	Up	100M/Full Duplex
LAN 4	Down	-
WLAN	Active	125M/G+

2.2.2 Administrator Access

- 1 For administrator access enter the default admin password **1234** to configure the wizards and the advanced features.
- 2 Click **Login** to proceed to a screen asking you to change your password or click **Cancel** to revert to the default password.
- 3 If you entered the admin password, it is highly recommended you change the default admin password! Enter a new password between 1 and 30 characters, retype it to confirm and click **Apply**. Alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.



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

Figure 10 Change Password at Login

ZyXEL

Use this screen to change the password.

Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess.

Enter your new password in the two fields below and click "Apply". Otherwise click "Ignore" to keep the default password

New Password:

Retype to Confirm:

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

Figure 11 Select a Mode

ZyXEL

Please select Wizard or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advanced features not included in Wizard mode.

Go to Wizard setup

Go to Advanced setup

Click here to always start with the Advanced setup.



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.

2.3 Resetting the ZyXEL Device

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

2.3.1 Using the Reset Button

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

2.4 Navigating the Web Configurator

2.4.1 Navigation Panel

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

Figure 12 Web Configurator: Main Screen

Use the submenus to configure ZyXEL Device features.

Click the Logout icon at any time to exit the web configurator.

Interface	Status	Rate
DSL	Down	0 kbps / 0 kbps
LAN 1	Down	-
LAN 2	Down	-
LAN 3	Up	100M/Full Duplex
LAN 4	Down	-
WLAN	Active	125M/G+



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

Table 3 Web Configurator Screens Summary



LINK/ICON	SUB-LINK	FUNCTION
Wizard 	INTERNET/WIRELESS SETUP	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
	BANDWIDTH MANAGEMENT SETUP	Use these screens to limit bandwidth usage by application or packet type.
Logout 		Click this icon to exit the web configurator.
Status		This screen shows the ZyXEL Device's general device, system and interface status information. Use this screen to access the summary statistics tables.
Network		
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to view and configure other connections for placing calls to another remote gateway.
	WAN Backup Setup	Use this screen to configure your traffic redirect properties and WAN backup settings.
LAN	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
	IP Alias	Use this screen to partition your LAN interface into subnets.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the ZyXEL Device.
	Address Mapping	Use this screen to configure network address translation mapping rules.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
Content Filter	Keyword	Use this screen to block sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the ZyXEL Device to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering on your ZyXEL Device.
Advanced		
Static Route		Use this screen to configure IP static routes.

Table 3 Web Configurator Screens Summary (continued)

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

2.4.2 Status Screen

The following summarizes how to navigate the web configurator from the **Status** screen. Some fields or links are not available if you entered the user password in the login password screen (see [Figure 9 on page 40](#)). Not all fields are available on all models.

Figure 13 Status Screen

Device Information

Host Name:
 Model Number: P-660HW-D1 v2
 MAC Address: 00:13:49:00:00:01
 ZyNOS Firmware Version: [V3.40\(ATA.0\)b2 | 1/24/2007](#)
 DSL Firmware Version: TI AR7 07.00.04.00

WAN Information

- DSL Mode: NORMAL
- IP Address: [0.0.0.0](#)
- IP Subnet Mask: 0.0.0.0
- Default Gateway: 0.0.0.0
- VPI/VCI: 8/35

LAN Information

- IP Address: [192.168.1.1](#)
- IP Subnet Mask: 255.255.255.0
- DHCP: [Server](#)

WLAN Information

- SSID: [ZyXEL](#)
- Channel: 6
- Security: Disabled

Security

- Firewall: [Enabled](#)
- Content Filter: [Disabled](#)

System Status

System Uptime: 0:08:07
 Current Date/Time: 01/01/2000 00:08:26
 System Mode: Routing / Bridging
 CPU Usage: 4.49%
 Memory Usage: 73%

Interface Status

Interface	Status	Rate
DSL	Down	0 kbps / 0 kbps
LAN 1	Down	-
LAN 2	Down	-
LAN 3	Up	100M/Full Duplex
LAN 4	Down	-
WLAN	Active	125M/G+

Summary

[AnyIP Table](#) [WLAN Status](#)
[Bandwidth Status](#) [Packet Statistics](#)

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

Table 4 Status Screen

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

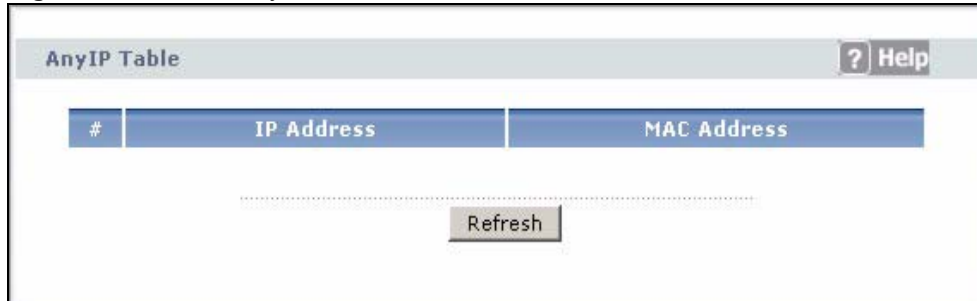
Table 4 Status Screen (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - Server , Relay or None .
WLAN Information (Wireless devices only)	
SSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN.
Channel	This is the channel number used by the ZyXEL Device now.
Security	This displays the level of wireless security the ZyXEL Device is using.
Security	
Firewall	This displays whether or not the ZyXEL Device's firewall is activated.
Content Filter	This displays whether or not the ZyXEL Device's content filtering is activated.
System Status	
System Uptime	This is the total time the ZyXEL Device has been on.
Current Date/ Time	This field displays your ZyXEL Device's present date and time.
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This number shows how many kilobytes of the heap memory the ZyXEL Device is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall. The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Memory Usage	This number shows the ZyXEL Device's total heap memory (in kilobytes). The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Interface Status	
Interface	This displays the ZyXEL Device port types.
Status	This field displays Down (line is down), Up (line is up or connected) if you're using Ethernet encapsulation and Down (line is down), Up (line is up or connected), Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE encapsulation.
Rate	For the LAN 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. For the WAN port, it displays the downstream and upstream transmission rate.
Summary	
Any IP Table	Use this screen to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the ZyXEL Device.
WLAN Status (Wireless devices only)	This screen displays the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device.
Bandwidth Status	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Packet Statistics	Use this screen to view port status and packet specific statistics.

2.4.3 Status: Any IP Table

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

Figure 14 Status: Any IP Table



The following table describes the labels in this screen.

Table 5 Status: Any IP Table

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

2.4.4 Status: WLAN Status

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

Figure 15 Status: WLAN Status



The following table describes the labels in this screen.

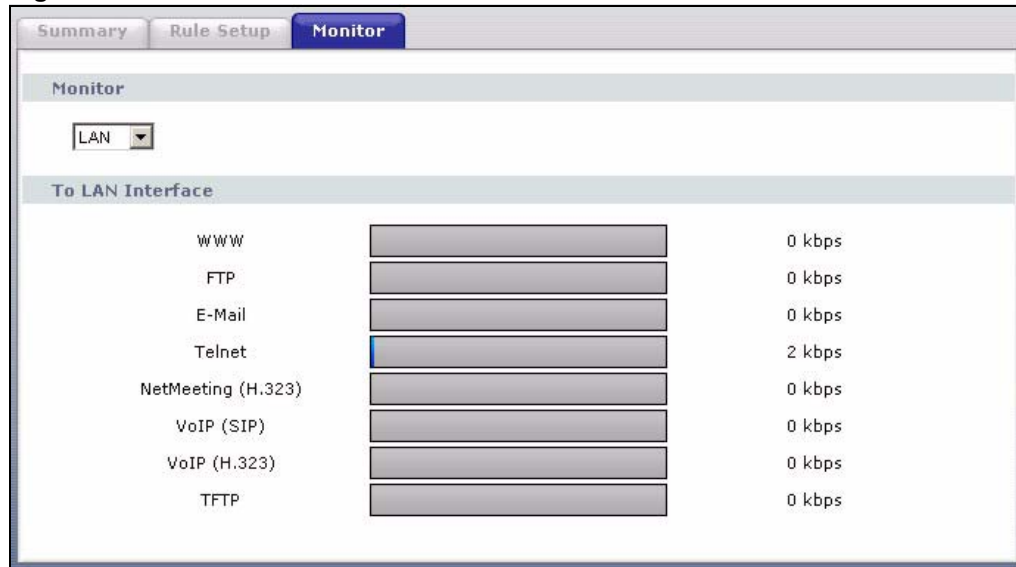
Table 6 Status: WLAN Status

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

2.4.5 Status: Bandwidth Status

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

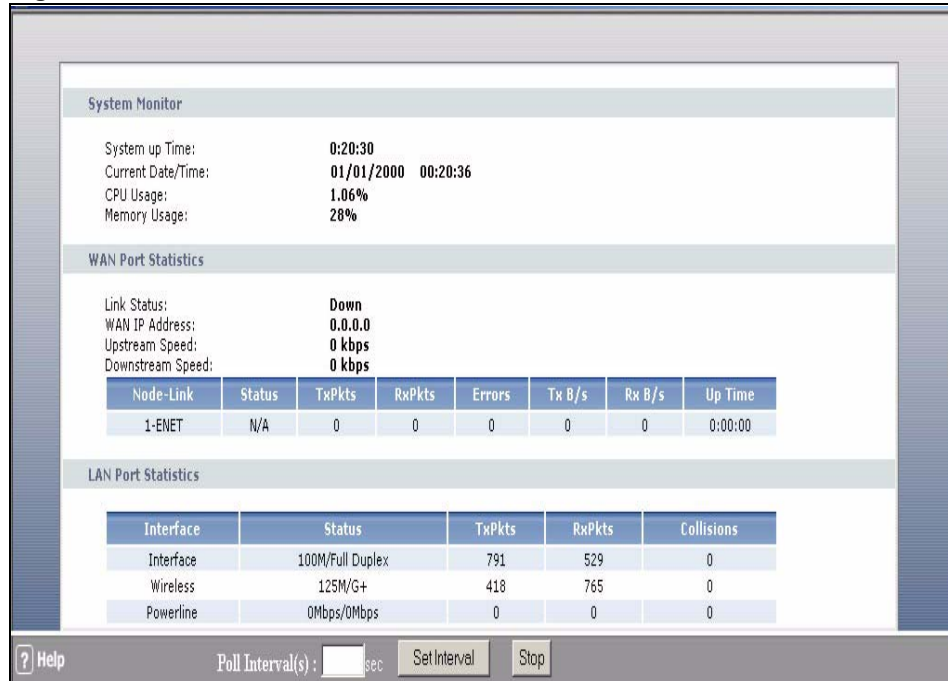
Figure 16 Status: Bandwidth Status



2.4.6 Status: Packet Statistics

Click the **Packet Statistics** hyperlink in the **Status** screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable. Not all fields are available on all models

Figure 17 Status: Packet Statistics



The following table describes the fields in this screen.

Table 7 Status: Packet Statistics

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

Table 7 Status: Packet Statistics (continued)

LABEL	DESCRIPTION
LAN Port Statistics	
Interface	This field displays the type of port.
Status	This field displays Down (line is down), Up (line is up or connected) if you're using Ethernet encapsulation and Down (line is down), Up (line is up or connected), Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval field above.
Stop	Click this button to halt the refreshing of the system statistics.

2.4.7 Changing Login Password

It is highly recommended that you periodically change the password for accessing the ZyXEL Device. If you didn't change the default one after you logged in or you want to change to a new password again, then click **Maintenance > System** to display the screen shown next. See [Table 90 on page 228](#) for detailed field descriptions.

Figure 18 System General

The screenshot shows the 'System General' configuration page. The 'General' tab is active. The 'System Setup' section includes fields for 'System Name', 'Domain Name', and 'Administrator Inactivity Timer' (set to 60 minutes). The 'Password' section is divided into 'User Password' and 'Admin Password'. The 'User Password' section is highlighted with a green rounded rectangle and contains 'New Password' and 'Retype to confirm' fields. Below the password fields is a 'Caution' message: 'Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.' At the bottom, there are 'Apply' and 'Cancel' buttons.

PART II

Wizards

Wizard Setup for Internet Access (53)

Bandwidth Management Wizard (67)

Wizard Setup for Internet Access

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

3.1 Introduction

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



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

3.2 Internet Access Wizard Setup


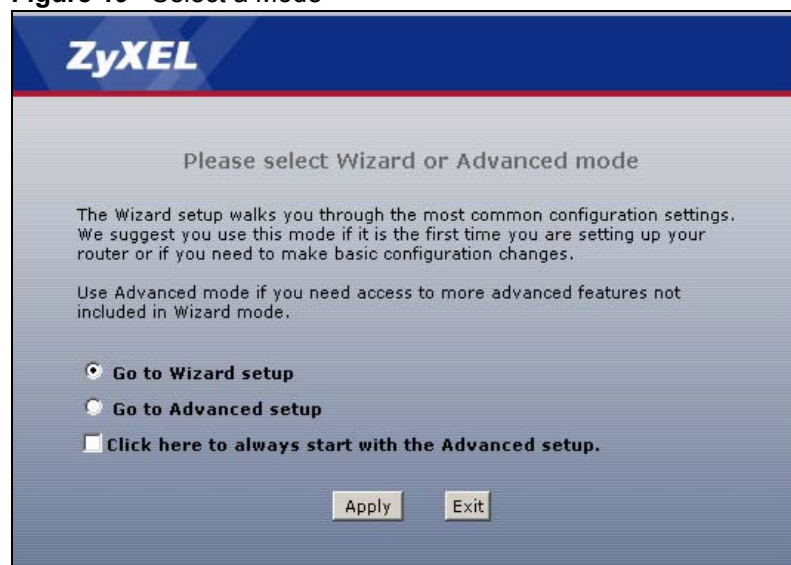
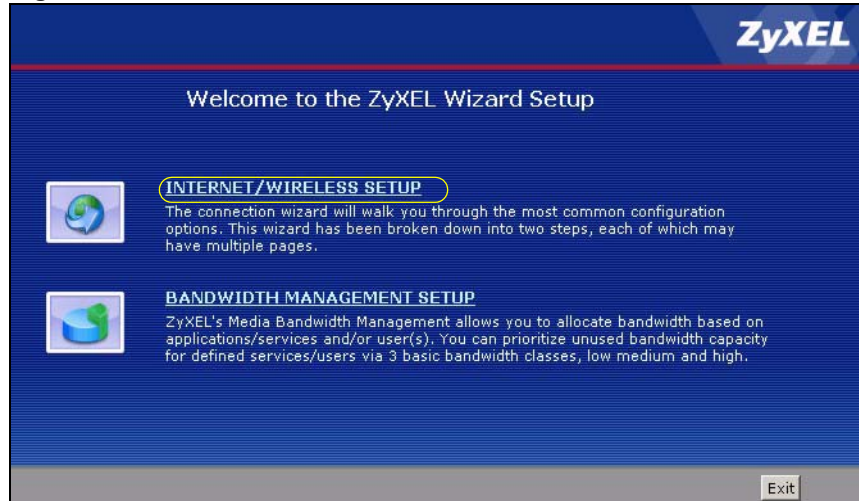
- 1 After you enter the admin password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon () in the top right corner of the web configurator to display the wizard main screen.

Figure 19 Select a Mode



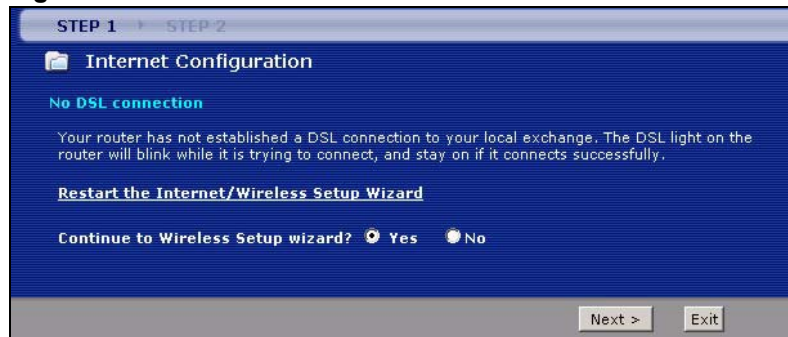
- 2 Click **INTERNET/WIRELESS SETUP** to configure the system for Internet access.

Figure 20 Wizard: Welcome



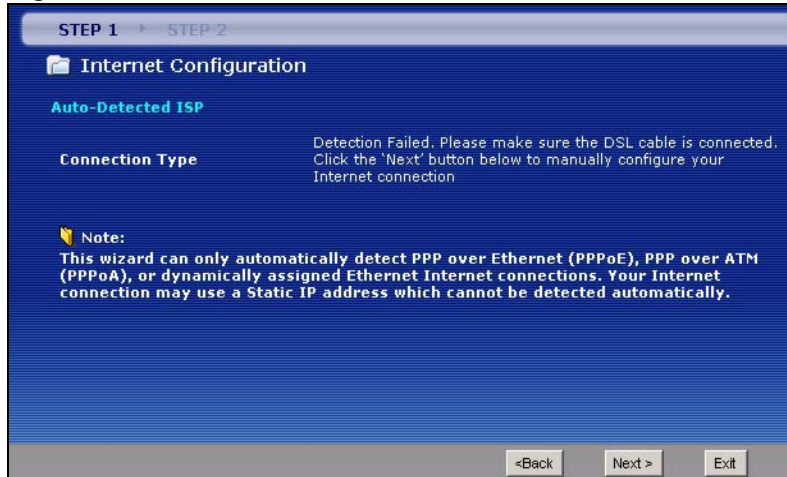
- 3 The wizard attempts to detect which WAN connection type you are using. If the wizard detects your connection type and your ISP uses PPPoE or PPPoA, go to [Section 3.2.1 on page 55](#). The screen varies depending on the connection type you use. If the wizard does not detect a connection type and the following screen appears (see [Figure 21 on page 54](#)), check your hardware connections and click **Restart the Internet/Wireless Setup Wizard** to have the ZyXEL Device detect your connection again.

Figure 21 Auto Detection: No DSL Connection



If the wizard still cannot detect a connection type and the following screen appears (see [Figure 22 on page 55](#)), click **Next** and refer to [Section 3.2.2 on page 55](#) on how to configure the ZyXEL Device for Internet access manually.

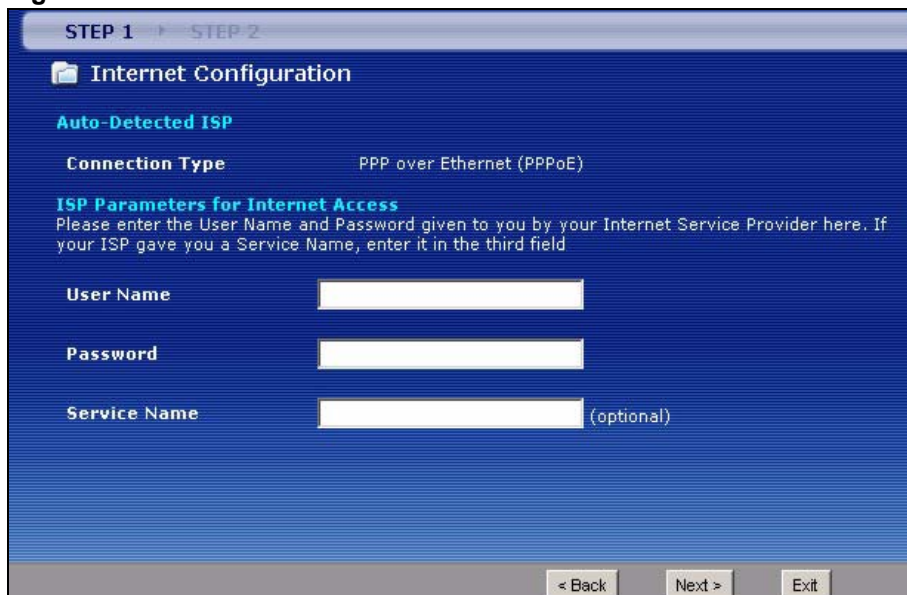
Figure 22 Auto Detection: Failed



3.2.1 Automatic Detection

- 1 If you have a PPPoE or PPPoA connection, a screen displays prompting you to enter your Internet account information. Enter the username, password and/or service name exactly as provided.
- 2 Click **Next**.

Figure 23 Auto-Detection: PPPoE



3.2.2 Manual Configuration

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

Figure 24 Internet Access Wizard Setup: ISP Parameters

STEP 1 **STEP 2**

Internet Configuration

ISP Parameters for Internet Access

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

Mode

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

Encapsulation

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

Multiplexing

Select the multiplexing type used by your ISP.

Virtual Circuit ID

VPI

VCI

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

The following table describes the fields in this screen.

Table 8 Internet Access Wizard Setup: ISP Parameters

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

- The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

Figure 25 Internet Connection with PPPoE

The following table describes the fields in this screen.

Table 9 Internet Connection with PPPoE

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

Figure 26 Internet Connection with RFC 1483

The following table describes the fields in this screen.

Table 10 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select Routing in the Mode field. Type your ISP assigned IP address in this field.
Back	Click Back to go back to the previous wizard screen.

Table 10 Internet Connection with RFC 1483 (continued)

LABEL	DESCRIPTION
Next	Click Next to continue to the next wizard screen.
Exit	Click Exit to close the wizard screen without saving your changes.

Figure 27 Internet Connection with ENET ENCAP

The following table describes the fields in this screen.

Table 11 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select Obtain an IP Address Automatically if you have a dynamic IP address.
Static IP Address	Select Static IP Address if your ISP gives you a fixed IP address.
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask if you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use ENET ENCAP in the Encapsulation field in the previous screen.
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes to the ZyXEL Device.
Exit	Click Exit to close the wizard screen without saving your changes.

Figure 28 Internet Connection with PPPoA

The following table describes the fields in this screen.

Table 12 Internet Connection with PPPoA

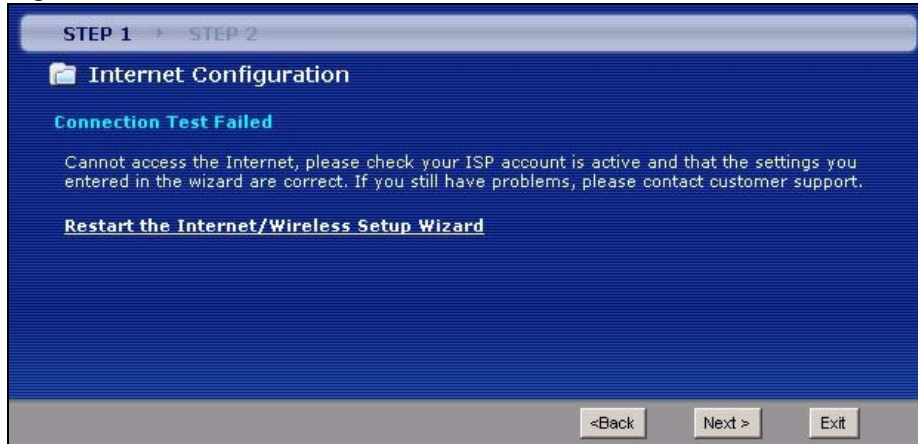
LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Back	Click Back to go back to the previous wizard screen.
Apply	Click Apply to save your changes to the ZyXEL Device.
Exit	Click Exit to close the wizard screen without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

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

Figure 29 Connection Test Failed-1

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

Figure 30 Connection Test Failed-2.

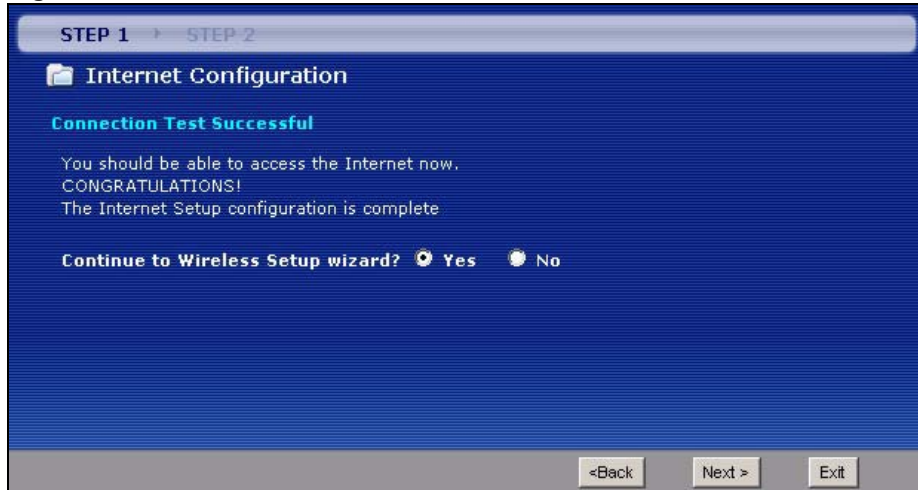


3.3 Wireless Connection Wizard Setup

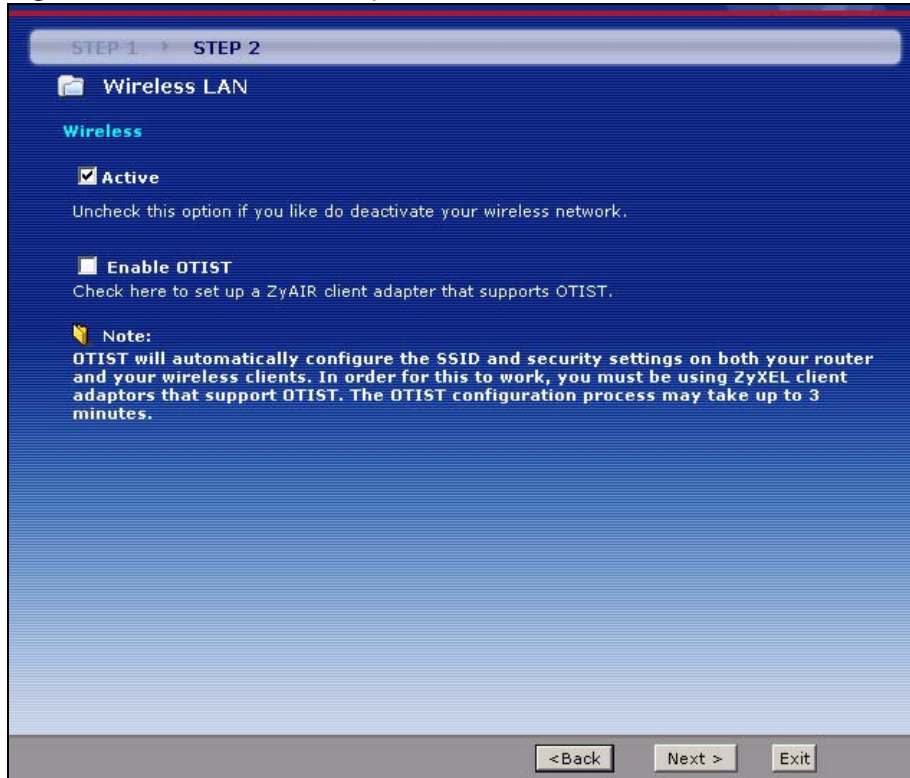
After you configure the Internet access information, use the following screens to set up your wireless LAN.

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

Figure 31 Connection Test Successful



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

Figure 32 Wireless LAN Setup Wizard 1

The following table describes the labels in this screen.

Table 13 Wireless LAN Setup Wizard 1

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

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

Figure 33 Wireless LAN Setup Wizard 2

STEP 1 ▶ STEP 2

Wireless LAN

Wireless

Network Name (SSID)
Give your network a name. You will search for this name from your wireless clients.

Channel Selection
Your router can use one of several channels. You should use the default channel unless other wireless networks nearby use the same channel.

Security
Use this option if you would prefer to create your own key, WPA is stronger than WEP but not all devices are compatible with WPA.

< Back Next > Exit

The following table describes the labels in this screen.

Table 14 Wireless LAN Setup Wizard 2

LABEL	DESCRIPTION
Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyXEL Device, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device.
Security	Select Automatically assign a WPA key (Recommended) to have the ZyXEL Device create a pre-shared key (WPA-PSK) automatically only if your wireless clients support WPA and OTIST. This option is available only when you enable OTIST in the previous wizard screen. Select Manually assign a WPA-PSK key to configure a pre-shared key (WPA-PSK). Choose this option only if your wireless clients support WPA. See Section 3.3.1 on page 63 for more information. Select Manually assign a WEP key to configure a WEP Key. See Section 3.3.2 on page 63 for more information. Select Disable wireless security to have no wireless LAN security configured and your network is accessible to any wireless networking device that is within range. Note: If you enable OTIST in the previous wizard screen but select Disable wireless security here, the ZyXEL Device still creates a pre-shared key (WPA-PSK) automatically. If you enable OTIST and select Manually assign a WEP key , the ZyXEL Device will replace the WEP key with a WPA-PSK.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.



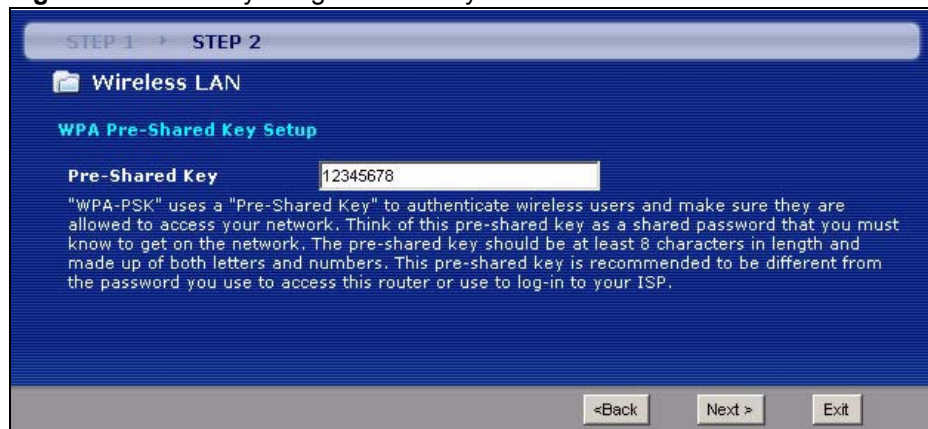
The wireless stations and ZyXEL Device must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) for wireless communication.

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

3.3.1 Manually assign a WPA-PSK key

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

Figure 34 Manually assign a WPA key



The following table describes the labels in this screen.

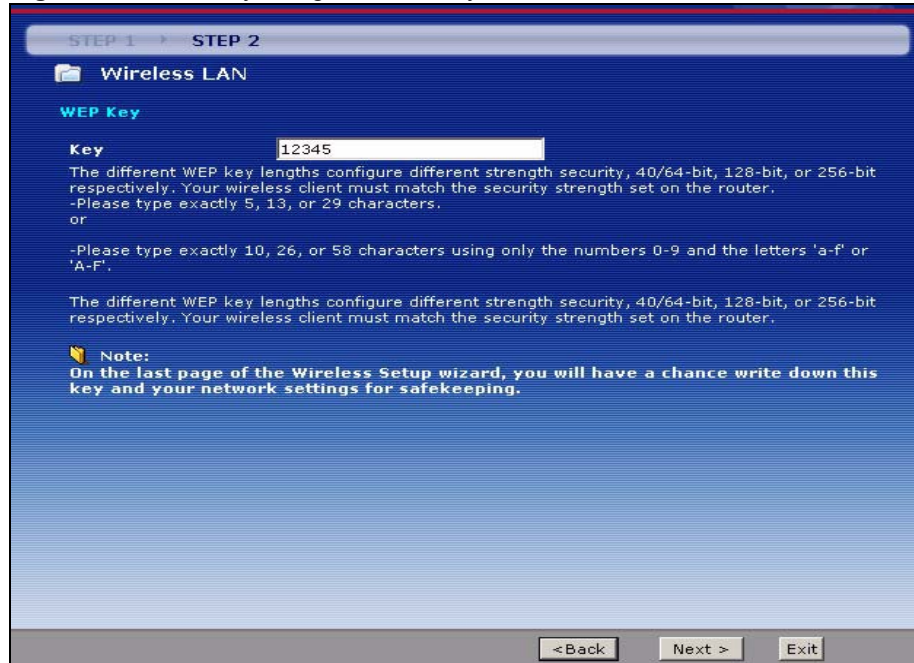
Table 15 Manually assign a WPA key

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

3.3.2 Manually assign a WEP key

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

Figure 35 Manually assign a WEP key



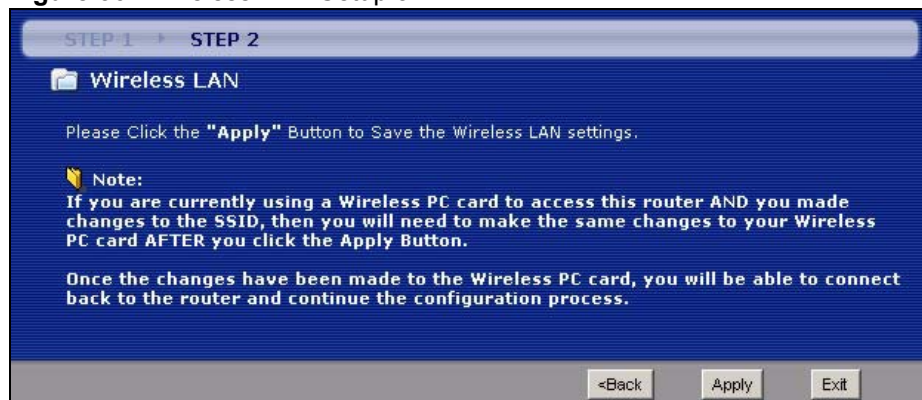
The following table describes the labels in this screen.

Table 16 Manually assign a WEP key

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

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

Figure 36 Wireless LAN Setup 3



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

Figure 37 Internet Access and WLAN Wizard Setup Complete



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

Bandwidth Management Wizard

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

4.1 Introduction

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

4.2 Predefined Media Bandwidth Management Services

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

Table 17 Media Bandwidth Management Setup: Services

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

Table 17 Media Bandwidth Management Setup: Services (continued)

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

4.3 Bandwidth Management Wizard Setup


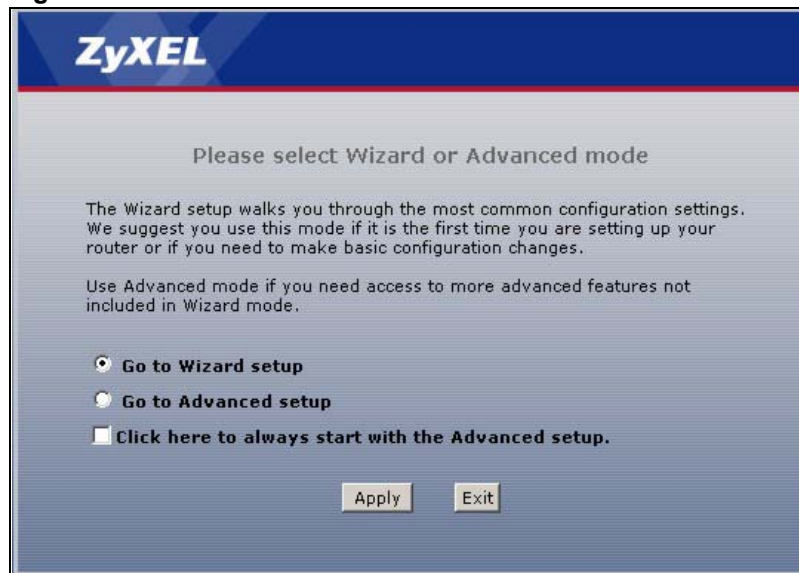
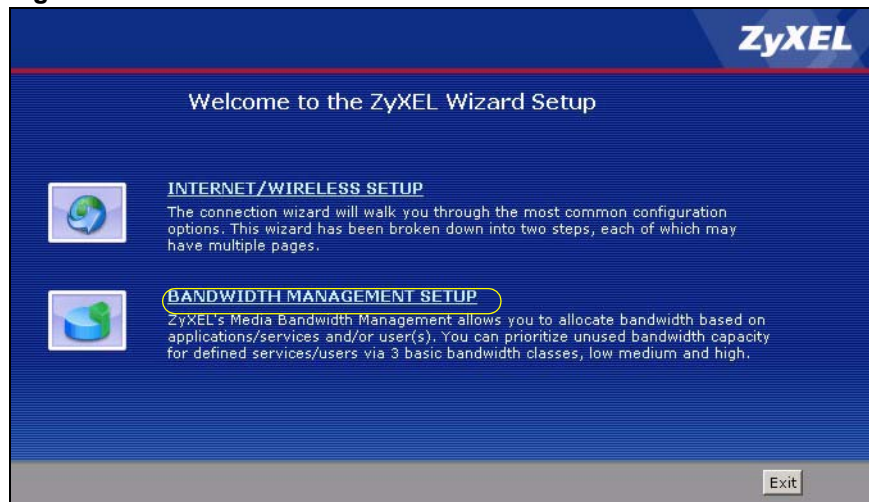
- 1 After you enter the admin password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon () in the top right corner of the web configurator to display the wizard main screen.

Figure 38 Select a Mode

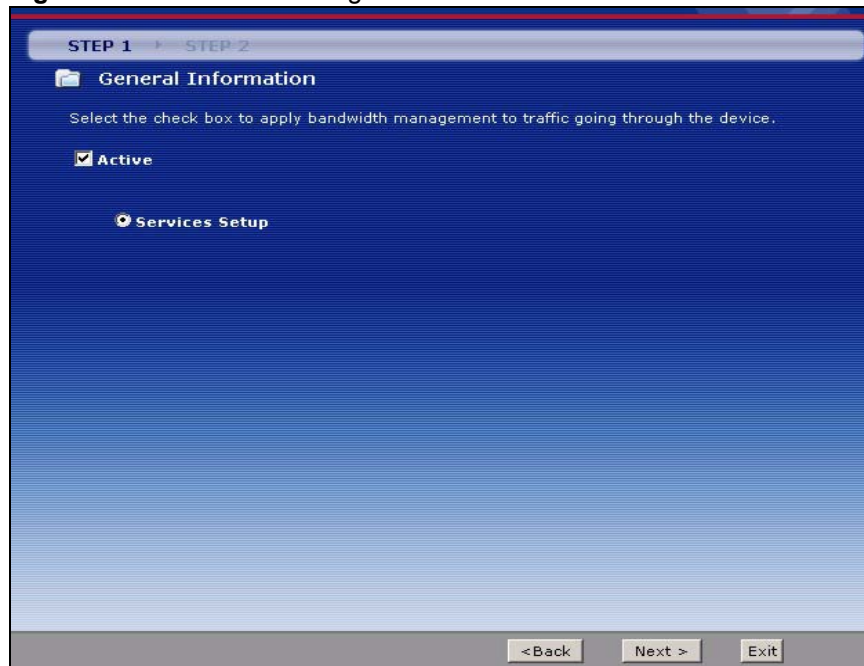
- Click **BANDWIDTH MANAGEMENT SETUP** to configure the system for Internet access.

Figure 39 Wizard: Welcome



- Activate bandwidth management and select to allocate bandwidth to packets based on the service requirements.

Figure 40 Bandwidth Management Wizard: General Information



The following fields describe the label in this screen.

Table 18 Bandwidth Management Wizard: General Information

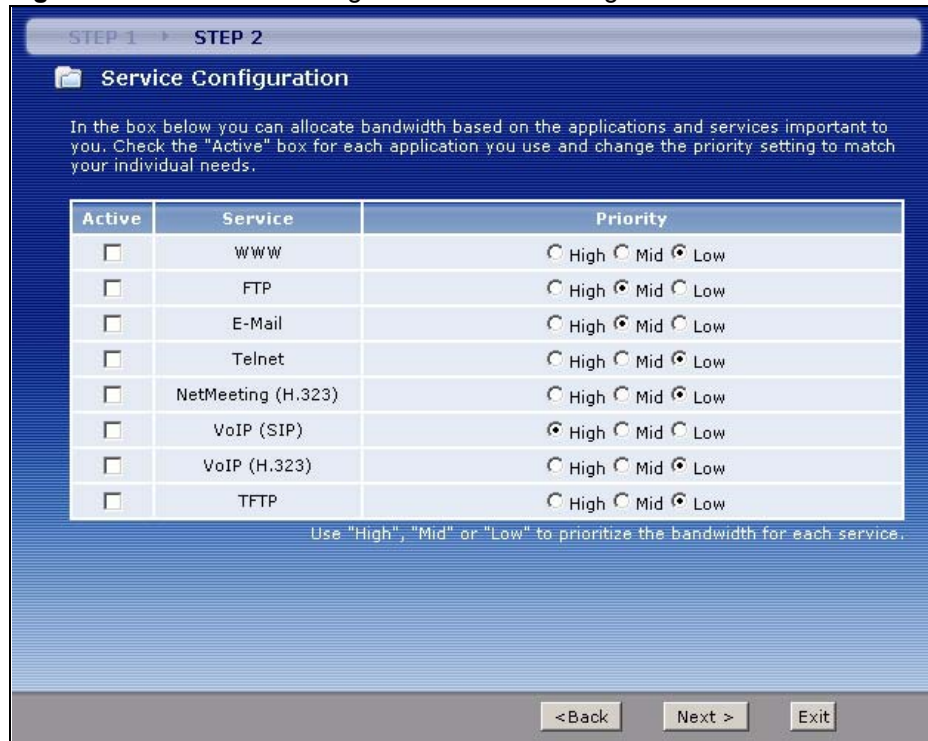
LABEL	DESCRIPTION
Active	Select the Active check box to have the ZyXEL Device apply bandwidth management to traffic going out through the ZyXEL Device's port(s). Select Services Setup to allocate bandwidth based on the service requirements.
Back	Click Back to display the previous screen.

Table 18 Bandwidth Management Wizard: General Information

LABEL	DESCRIPTION
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

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

Figure 41 Bandwidth Management Wizard: Configuration



The following table describes the labels in this screen.

Table 19 Bandwidth Management Wizard: Configuration

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

Table 19 Bandwidth Management Wizard: Configuration

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

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

Figure 42 Bandwidth Management Wizard: Complete

PART III

Network

WAN Setup (75)

LAN Setup (93)

Wireless LAN (105)

Network Address Translation (NAT) Screens (129)

WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

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

5.1.1 Encapsulation

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

5.1.1.1 ENET ENCAP

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

5.1.1.2 PPP over Ethernet

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

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

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

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

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

5.1.1.3 PPPoA

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

5.1.1.4 RFC 1483

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

5.1.2 Multiplexing

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

5.1.2.1 VC-based Multiplexing

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

5.1.2.2 LLC-based Multiplexing

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

5.1.3 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. Consult your telephone company for information on encapsulation and multiplexing methods for LAN-to-LAN applications, for example between a branch office and corporate headquarters. There must be prior agreement on encapsulation and multiplexing methods because they cannot be automatically determined. What method(s) you use also depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

5.1.3.1 Scenario 1: One VC, Multiple Protocols

PPPoA (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

5.1.3.2 Scenario 2: One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPPoA** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

5.1.3.3 Scenario 3: Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select RFC-1483 encapsulation and VC-based multiplexing.

5.1.4 VPI and VCI

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

5.1.5 IP Address Assignment

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

5.1.5.1 IP Assignment with PPPoA or PPPoE Encapsulation

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

5.1.5.2 IP Assignment with RFC 1483 Encapsulation

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

5.1.5.3 IP Assignment with ENET ENCAP Encapsulation

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

5.1.6 Nailed-Up Connection (PPP)

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

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

5.1.7 NAT

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

5.2 Metric

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

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

- Normal route: designated by the ISP (see [Section 5.5 on page 80](#))
- Traffic-redirect route (see [Section 5.7 on page 89](#))
- WAN-backup route, also called dial-backup (see [Section 5.8 on page 89](#))

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

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

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

5.3 Traffic Shaping

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

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

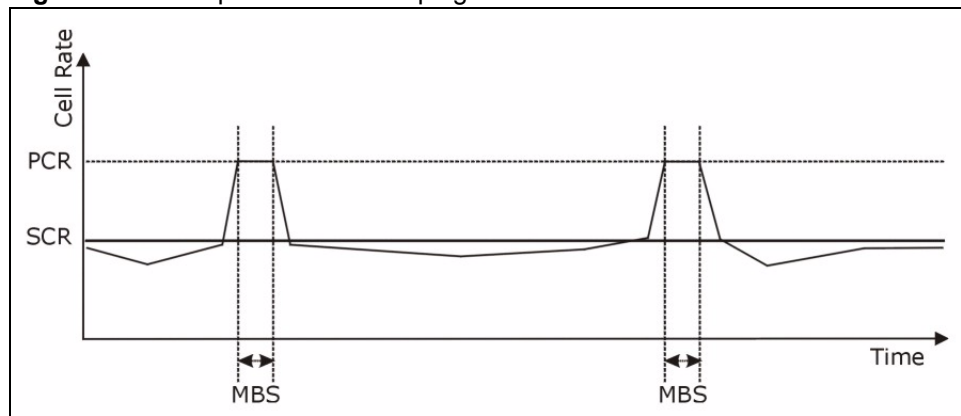
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

Figure 43 Example of Traffic Shaping



5.3.1 ATM Traffic Classes

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

5.3.1.1 Constant Bit Rate (CBR)

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

5.3.1.2 Variable Bit Rate (VBR)

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

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

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

5.3.1.3 Unspecified Bit Rate (UBR)

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

5.4 Zero Configuration Internet Access

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

Zero configuration for Internet access is disable when

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

5.5 Internet Connection

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

See [Section 5.1 on page 75](#) for more information.

Figure 44 Internet Connection (PPPoE)

The following table describes the labels in this screen.

Table 20 Internet Connection

LABEL	DESCRIPTION
General	
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select Routing (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.

Table 20 Internet Connection (continued)

LABEL	DESCRIPTION
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	This option is available if you select Routing in the Mode field.
Obtain an IP Address Automatically	Select this if you get a dynamic IP address from your Internet Service Provider (ISP). A dynamic IP address is not fixed; your ISP assigns you a different one each time you connect to the Internet. This option is not available if you select RFC 1483 in the Encapsulation field.
Static IP Address	Select this if your ISP gave you a fixed IP address. Enter the IP address you were given in the IP Address field.
IP Address	If your ISP gave you an IP address to use, enter it here.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
Gateway IP address (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select ENET ENCAP in the Encapsulation field
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session will not timeout.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.
Advanced Setup	Click this button to display the Advanced Internet Connection Setup screen and edit more details of your WAN setup.

5.5.1 Configuring Advanced Internet Connection Setup

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

Figure 45 Advanced Internet Connection Setup

The following table describes the labels in this screen.

Table 21 Advanced Internet Connection Setup

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

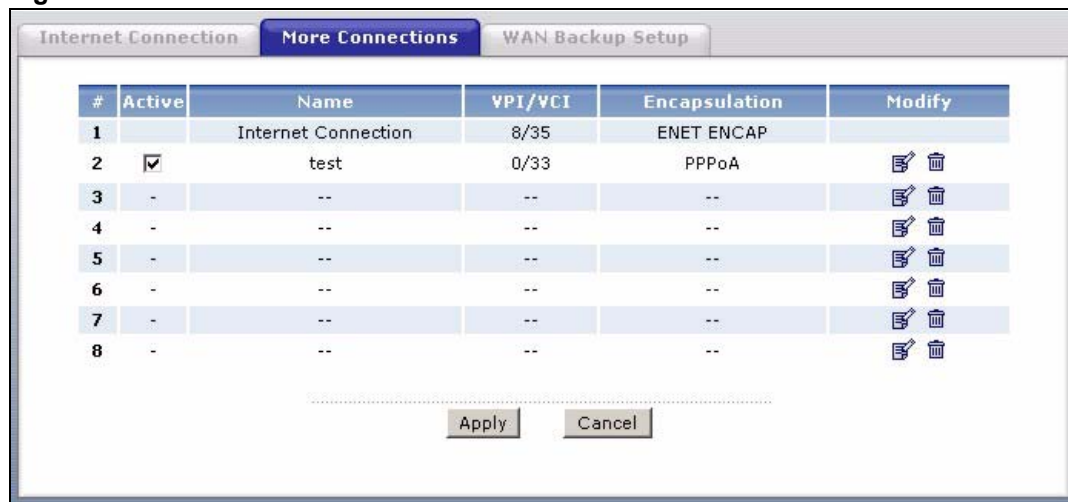
Table 21 Advanced Internet Connection Setup (continued)

LABEL	DESCRIPTION
Zero Configuration	This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode. Select Yes to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes. Select No to disable this feature. You must manually configure the ZyXEL Device for Internet access.
PPPoE Passthrough	This feature is available when you select PPPoE encapsulation. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

5.6 Configuring More Connections

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

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

Figure 46 More Connections

The following table describes the labels in this screen.

Table 22 More Connections

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

5.6.1 More Connections Edit

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

Figure 47 More Connections Edit

General	
<input checked="" type="checkbox"/> Active	
Name:	<input type="text" value="ChangeMe"/>
Mode	<input type="text" value="Routing"/>
Encapsulation	<input type="text" value="PPPoA"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Multiplexing	<input type="text" value="VC"/>
VPI	<input type="text" value="0"/>
VCI	<input type="text" value="33"/>
IP Address	
<input type="radio"/> Obtain an IP Address Automatically	
<input checked="" type="radio"/> Static IP Address	
IP Address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="0.0.0.0"/>
Gateway IP Address	<input type="text" value="0.0.0.0"/>
Connection	
<input type="radio"/> Nailed-Up Connection	
<input checked="" type="radio"/> Connect on Demand	
Max Idle timeout	<input type="text" value="0"/> sec
NAT	
<input type="radio"/> None	
<input checked="" type="radio"/> SUA Only Edit	
<input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>	

The following table describes the labels in this screen.

Table 23 More Connections Edit

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

Table 23 More Connections Edit (continued)

LABEL	DESCRIPTION
Multiplexing	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC.</p> <p>By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol.</p> <p>For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.</p>
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	This option is available if you select Routing in the Mode field.
Obtain an IP Address Automatically	<p>Select this if you get a dynamic IP address from your Internet Service Provider (ISP). A dynamic IP address is not fixed; your ISP assigns you a different one each time you connect to the Internet.</p> <p>This option is not available if you select RFC 1483 in the Encapsulation field.</p>
Static IP Address	Select this if your ISP gave you a fixed IP address. Enter the IP address you were given in the IP Address field.
IP Address	If your ISP gave you an IP address to use, enter it here.
Subnet Mask	<p>Enter a subnet mask in dotted decimal notation.</p> <p>Refer to the appendices to calculate a subnet mask If you are implementing subnetting.</p>
Gateway IP address	Specify a gateway IP address (supplied by your ISP).
Connection	
Nailed-Up Connection	Select Nailed-Up Connection when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session will not timeout.
NAT	NAT is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.
None	Select None to disable NAT.
SUA Only	<p>SUA only is available only when you select Routing in the Mode field.</p> <p>Select SUA Only if you have one public IP address and want to use NAT. Click Edit to go to the Port Forwarding screen to edit a server mapping set.</p>
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.
Advanced Setup	Click this button to display the More Connections Advanced screen and edit more details of your WAN setup.

5.6.2 Configuring More Connections Advanced Setup

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

Figure 48 More Connections Advanced Setup

The following table describes the labels in this screen.

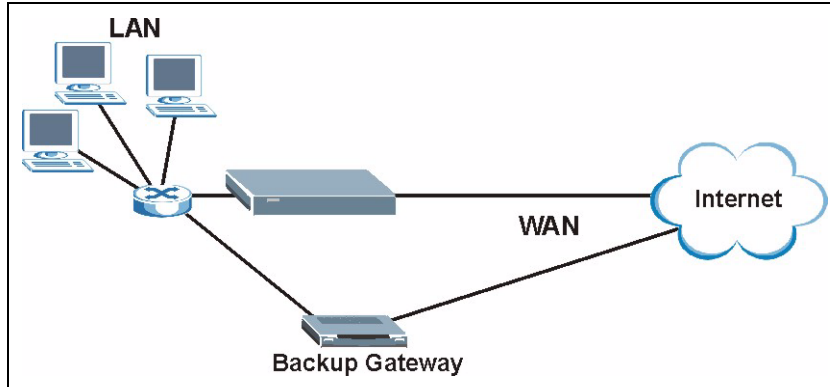
Table 24 More Connections Advanced Setup

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

5.7 Traffic Redirect

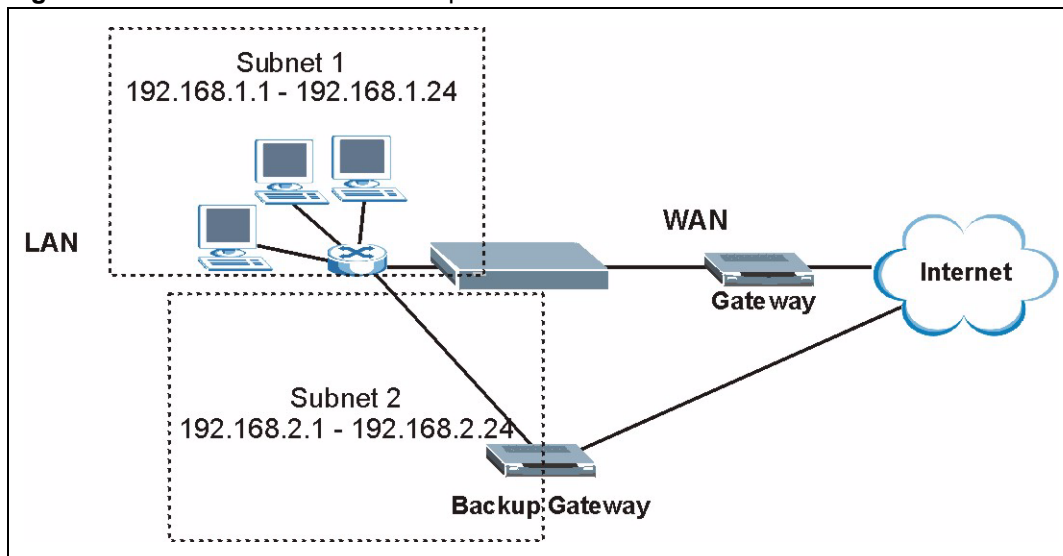
Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet. An example is shown in the figure below.

Figure 49 Traffic Redirect Example



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

Figure 50 Traffic Redirect LAN Setup



5.8 Configuring WAN Backup

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

Figure 51 WAN Backup Setup

The following table describes the labels in this screen.

Table 25 WAN Backup Setup

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

Table 25 WAN Backup Setup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the Check WAN IP Address field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the Fail Tolerance field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.
Active Traffic Redirect	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

LAN Setup

This chapter describes how to configure LAN settings.

6.1 LAN Overview

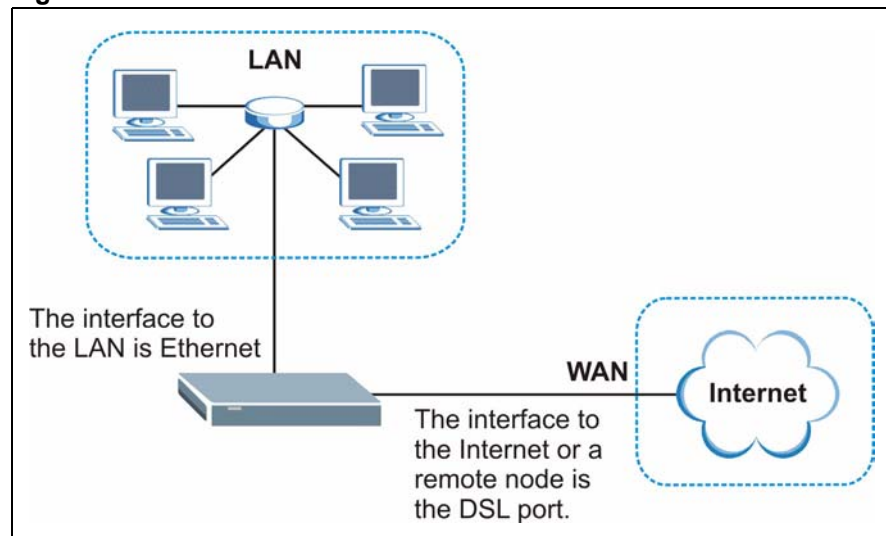
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 6.3 on page 98](#) to configure the LAN screens.

6.1.1 LANs, WANs and the ZyXEL Device

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

Figure 52 LAN and WAN IP Addresses



6.1.2 DHCP Setup

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

6.1.2.1 IP Pool Setup

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

6.1.3 DNS Server Address

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

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

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

If the **Primary** and **Secondary DNS Server** fields in the **DHCP Setup** screen are not specified, for instance, left as **0.0.0.0**, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

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

6.1.4 DNS Server Address Assignment

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

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in the **DHCP Setup** screen.
- The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left as **0.0.0.0** in the **DHCP Setup** screen.

6.2 LAN TCP/IP

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

6.2.1 IP Address and Subnet Mask

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

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

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

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

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

6.2.1.1 Private IP Addresses

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

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

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



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

6.2.2 RIP Setup

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

When set to:

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

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

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

6.2.3 Multicast

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

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address

224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

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

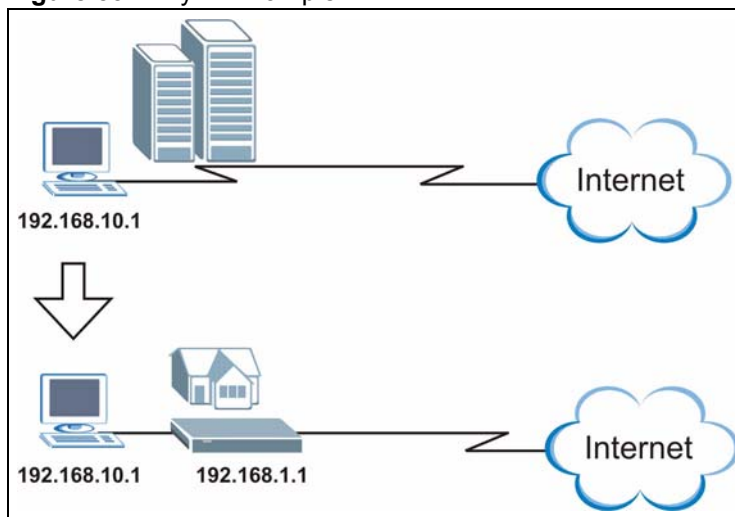
6.2.4 Any IP

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

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

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

Figure 53 Any IP Example



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



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

6.2.4.1 How Any IP Works

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

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

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

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

6.3 Configuring LAN IP

Click **LAN** to open the **IP** screen. See [Section 6.1 on page 93](#) for background information.

Figure 54 LAN IP

LAN TCP/IP	
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>	

The following table describes the fields in this screen.

Table 26 LAN IP

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

6.3.1 Configuring Advanced LAN Setup

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

Figure 55 Advanced LAN Setup

The following table describes the labels in this screen.

Table 27 Advanced LAN Setup

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

Table 27 Advanced LAN Setup (continued)

LABEL	DESCRIPTION
Any IP Setup	Select the Active check box to enable the Any IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyXEL Device's LAN IP address can connect to the ZyXEL Device or access the Internet through the ZyXEL Device.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.4 DHCP Setup

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

Figure 56 DHCP Setup

The screenshot shows the DHCP Setup configuration interface. It includes a navigation bar with tabs for IP, DHCP Setup, Client List, and IP Alias. The DHCP Setup section contains the following fields:

- DHCP: Server (dropdown menu)
- IP Pool Starting Address: 192.168.1.33
- Pool Size: 32
- Remote DHCP Server: 0.0.0.0

The DNS Server section contains the following fields:

- DNS Servers Assigned by DHCP Server:
 - Primary DNS Server: 0.0.0.0
 - Secondary DNS Server: 0.0.0.0

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