

# *NBG-334SH*

*802.11g Super G High Power Wireless Router*

## *User's Guide*

Version 3.60

01/2007

Edition 1





# 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](http://www.zyxel.com) for additional support documentation and product certifications.

## User Guide Feedback

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

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

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

# Document Conventions

## Warnings and Notes

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



---

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

---



---

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










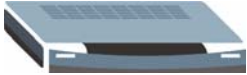
---

## Syntax Conventions

- The NBG-334SH may be referred to as the “ZyXEL Device”, the “device”, the “product” 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 
Modem 		

# Safety Warnings



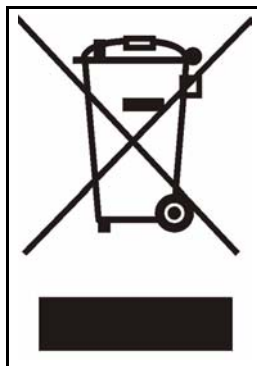
---

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.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.







# Contents Overview

<b>Introduction .....</b>	<b>27</b>
Getting to Know Your ZyXEL Device .....	29
Wireless Tutorial .....	33
Introducing the Web Configurator .....	41
<b>Wizard .....</b>	<b>53</b>
Connection Wizard .....	55
<b>Advanced .....</b>	<b>71</b>
Wireless LAN .....	73
WAN .....	89
LAN .....	99
DHCP Server .....	105
Network Address Translation (NAT) .....	109
Dynamic DNS .....	119
Firewall .....	121
Content Filtering .....	127
Static Route Screens .....	133
Bandwidth Management .....	137
Remote Management Screens .....	149
Universal Plug-and-Play (UPnP) .....	155
<b>Maintenance and Troubleshooting .....</b>	<b>167</b>
System .....	169
Logs .....	173
Tools .....	187
Configuration Mode .....	193
Troubleshooting .....	195
<b>Appendices and Index .....</b>	<b>201</b>



# Table of Contents

<b>About This User's Guide .....</b>	<b>3</b>
<b>Document Conventions.....</b>	<b>4</b>
<b>Safety Warnings.....</b>	<b>6</b>
<b>Contents Overview .....</b>	<b>9</b>
<b>Table of Contents.....</b>	<b>11</b>
<b>List of Figures .....</b>	<b>19</b>
<b>List of Tables.....</b>	<b>23</b>
<b>Part I: Introduction.....</b>	<b>27</b>
<b>Chapter 1</b>	
<b>Getting to Know Your ZyXEL Device .....</b>	<b>29</b>
1.1 ZyXEL Device Overview .....	29
1.2 Applications for the ZyXEL Device .....	29
1.2.1 Secure Broadband Internet Access .....	29
1.3 Ways to Manage the ZyXEL Device .....	30
1.4 Good Habits for Managing the ZyXEL Device .....	30
1.5 LEDs .....	31
<b>Chapter 2</b>	
<b>Wireless Tutorial .....</b>	<b>33</b>
2.1 Example Parameters .....	33
2.2 Configuring the AP .....	33
2.3 Configuring the Wireless Client .....	35
2.3.1 Connecting to a Wireless LAN .....	36
2.3.2 Creating and Using a Profile .....	38
<b>Chapter 3</b>	
<b>Introducing the Web Configurator .....</b>	<b>41</b>
3.1 Web Configurator Overview .....	41
3.2 Accessing the Web Configurator .....	41
3.3 Resetting the ZyXEL Device .....	43
3.3.1 Procedure to Use the Reset Button .....	43

3.4 Navigating the Web Configurator .....	43
3.4.1 The Status Screen .....	43
3.4.2 Navigation Panel .....	46
3.5 Summary: Any IP Table .....	48
3.5.1 Summary: Bandwidth Management Monitor .....	48
3.5.2 Summary: DHCP Table .....	49
3.5.3 Summary: Packet Statistics .....	50
3.5.4 Summary: Wireless Station Status .....	50
<b>Part II: Wizard .....</b>	<b>53</b>
<b>Chapter 4</b>	
<b>Connection Wizard .....</b>	<b>55</b>
4.1 Wizard Setup .....	55
4.2 Connection Wizard: STEP 1: System Information .....	56
4.2.1 System Name .....	56
4.2.2 Domain Name .....	57
4.3 Connection Wizard: STEP 2: Wireless LAN .....	57
4.3.1 Basic (WEP) Security .....	59
4.3.2 Extend (WPA-PSK or WPA2-PSK) Security .....	60
4.4 Connection Wizard: STEP 3: Internet Configuration .....	60
4.4.1 Ethernet Connection .....	61
4.4.2 PPPoE Connection .....	61
4.4.3 PPTP Connection .....	62
4.4.4 Your IP Address .....	64
4.4.5 WAN IP Address Assignment .....	64
4.4.6 IP Address and Subnet Mask .....	65
4.4.7 DNS Server Address Assignment .....	65
4.4.8 WAN IP and DNS Server Address Assignment .....	66
4.4.9 WAN MAC Address .....	67
4.5 Connection Wizard: STEP 4: Bandwidth management .....	68
4.6 Connection Wizard Complete .....	68
<b>Part III: Advanced .....</b>	<b>71</b>
<b>Chapter 5</b>	
<b>Wireless LAN .....</b>	<b>73</b>
5.1 Wireless Network Overview .....	73
5.2 Wireless Security Overview .....	74
5.2.1 SSID .....	74

5.2.2 MAC Address Filter .....	74
5.2.3 User Authentication .....	74
5.2.4 Encryption .....	75
5.3 Quality of Service .....	76
5.3.1 WMM QoS .....	76
5.4 General Wireless LAN Screen .....	77
5.4.1 No Security .....	78
5.4.2 WEP Encryption .....	78
5.4.3 WPA-PSK/WPA2-PSK .....	80
5.4.4 WPA/WPA2 .....	81
5.5 MAC Filter .....	83
5.6 Wireless LAN Advanced Screen .....	84
5.7 Quality of Service (QoS) Screen .....	85
5.7.1 Application Priority Configuration .....	87
<b>Chapter 6</b>	
<b>WAN.....</b>	<b>89</b>
6.1 WAN Overview .....	89
6.2 WAN MAC Address .....	89
6.3 Multicast .....	89
6.4 Internet Connection .....	90
6.4.1 Ethernet Encapsulation .....	90
6.4.2 PPPoE Encapsulation .....	92
6.4.3 PPTP Encapsulation .....	94
6.5 Advanced WAN Screen .....	97
<b>Chapter 7</b>	
<b>LAN.....</b>	<b>99</b>
7.1 LAN Overview .....	99
7.1.1 IP Pool Setup .....	99
7.1.2 System DNS Servers .....	99
7.2 LAN TCP/IP .....	99
7.2.1 Factory LAN Defaults .....	99
7.2.2 IP Address and Subnet Mask .....	100
7.2.3 Multicast .....	100
7.2.4 Any IP .....	100
7.3 LAN IP Screen .....	102
7.4 LAN IP Alias .....	102
7.5 Advanced LAN Screen .....	103
<b>Chapter 8</b>	
<b>DHCP Server.....</b>	<b>105</b>
8.1 DHCP .....	105

8.2 DHCP Server General Screen .....	105
8.3 DHCP Server Advanced Screen .....	106
8.4 Client List Screen .....	107
<b>Chapter 9</b>	
<b>Network Address Translation (NAT).....</b>	<b>109</b>
9.1 NAT Overview .....	109
9.2 Using NAT .....	109
9.2.1 Port Forwarding: Services and Port Numbers .....	109
9.2.2 Configuring Servers Behind Port Forwarding Example .....	110
9.3 General NAT Screen .....	110
9.4 NAT Application Screen .....	111
9.4.1 Game List Example .....	113
9.5 Trigger Port Forwarding .....	114
9.5.1 Trigger Port Forwarding Example .....	114
9.5.2 Two Points To Remember About Trigger Ports .....	115
9.6 NAT Advanced Screen .....	115
<b>Chapter 10</b>	
<b>Dynamic DNS .....</b>	<b>119</b>
10.1 Dynamic DNS Introduction .....	119
10.1.1 DynDNS Wildcard .....	119
10.2 Dynamic DNS Screen .....	119
<b>Chapter 11</b>	
<b>Firewall.....</b>	<b>121</b>
11.1 Introduction to ZyXEL's Firewall .....	121
11.1.1 What is a Firewall? .....	121
11.1.2 Stateful Inspection Firewall .....	121
11.1.3 About the ZyXEL Device Firewall .....	121
11.1.4 Guidelines For Enhancing Security With Your Firewall .....	122
11.2 Triangle Routes .....	122
11.2.1 Triangle Routes and IP Alias .....	122
11.3 General Firewall Screen .....	123
11.4 Services Screen .....	124
<b>Chapter 12</b>	
<b>Content Filtering .....</b>	<b>127</b>
12.1 Introduction to Content Filtering .....	127
12.2 Restrict Web Features .....	127
12.3 Days and Times .....	127
12.4 Filter Screen .....	127
12.5 Schedule .....	129

12.6 Customizing Keyword Blocking URL Checking .....	130
12.6.1 Domain Name or IP Address URL Checking .....	130
12.6.2 Full Path URL Checking .....	130
12.6.3 File Name URL Checking .....	130
<b>Chapter 13</b>	
<b>Static Route Screens .....</b>	<b>133</b>
13.1 Static Route Overview .....	133
13.2 IP Static Route Screen .....	133
13.2.1 Static Route Setup Screen .....	134
<b>Chapter 14</b>	
<b>Bandwidth Management.....</b>	<b>137</b>
14.1 Bandwidth Management Overview .....	137
14.2 Application-based Bandwidth Management .....	137
14.3 Subnet-based Bandwidth Management .....	137
14.4 Application and Subnet-based Bandwidth Management .....	138
14.5 Bandwidth Management Priorities .....	138
14.6 Predefined Bandwidth Management Services .....	139
14.6.1 Services and Port Numbers .....	140
14.7 Default Bandwidth Management Classes and Priorities .....	142
14.8 Bandwidth Management General Configuration .....	142
14.9 Bandwidth Management Advanced Configuration .....	143
14.9.1 Rule Configuration with the Pre-defined Service .....	144
14.9.2 Rule Configuration with the User-defined Service .....	145
14.10 Bandwidth Management Monitor .....	146
<b>Chapter 15</b>	
<b>Remote Management Screens.....</b>	<b>149</b>
15.1 Remote Management Overview .....	149
15.1.1 Remote Management Limitations .....	150
15.1.2 Remote Management and NAT .....	150
15.1.3 System Timeout .....	150
15.2 WWW Screen .....	150
15.3 Telnet .....	151
15.4 Telnet Screen .....	151
15.5 FTP Screen .....	152
15.6 DNS Screen .....	153
<b>Chapter 16</b>	
<b>Universal Plug-and-Play (UPnP).....</b>	<b>155</b>
16.1 Introducing Universal Plug and Play .....	155
16.1.1 How do I know if I'm using UPnP? .....	155

16.1.2 NAT Traversal .....	155
16.1.3 Cautions with UPnP .....	155
16.2 UPnP and ZyXEL .....	156
16.3 UPnP Screen .....	156
16.4 Installing UPnP in Windows Example .....	157
<b>Part IV: Maintenance and Troubleshooting .....</b>	<b>167</b>
<b>Chapter 17</b>	
<b>System .....</b>	<b>169</b>
17.1 System Overview .....	169
17.2 System General Screen .....	169
17.3 Time Setting Screen .....	170
<b>Chapter 18</b>	
<b>Logs .....</b>	<b>173</b>
18.1 View Log .....	173
18.2 Log Settings .....	174
18.3 Log Descriptions .....	177
<b>Chapter 19</b>	
<b>Tools.....</b>	<b>187</b>
19.1 Firmware Upload Screen .....	187
19.2 Configuration Screen .....	188
19.2.1 Backup Configuration .....	189
19.2.2 Restore Configuration .....	189
19.2.3 Back to Factory Defaults .....	190
19.3 Restart Screen .....	190
<b>Chapter 20</b>	
<b>Configuration Mode .....</b>	<b>193</b>
<b>Chapter 21</b>	
<b>Troubleshooting.....</b>	<b>195</b>
21.1 Power, Hardware Connections, and LEDs .....	195
21.2 ZyXEL Device Access and Login .....	196
21.3 Internet Access .....	197
21.4 Resetting the ZyXEL Device to Its Factory Defaults .....	199
21.5 Advanced Features .....	199
<b>Part V: Appendices and Index .....</b>	<b>201</b>



---

Appendix A Product Specifications.....	203
Appendix B Pop-up Windows, JavaScripts and Java Permissions .....	207
Appendix C IP Addresses and Subnetting .....	213
Appendix D Wall-mounting Instructions.....	221
Appendix E Setting up Your Computer's IP Address.....	223
21.5.1 Verifying Settings .....	238
Appendix F Wireless LANs.....	239
21.5.2 WPA(2)-PSK Application Example .....	248
21.5.3 WPA(2) with RADIUS Application Example .....	248
Appendix G Command Interpreter .....	251
Appendix H NetBIOS Filter Commands .....	255
Appendix I Services.....	257
Appendix J Internal SPTGEN.....	261
Appendix K Legal Information .....	277
Appendix L Customer Support .....	281
<b>Index.....</b>	<b>285</b>



# List of Figures

Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem .....	30
Figure 2 WLAN Application Example .....	30
Figure 3 Front Panel .....	31
Figure 4 AP: Wireless LAN > General .....	34
Figure 5 AP: Status .....	35
Figure 6 AP: Status: WLAN Station Status .....	35
Figure 7 ZyXEL Utility: Security Settings .....	37
Figure 8 ZyXEL Utility: Confirm Save .....	37
Figure 9 ZyXEL Utility: Link Info .....	37
Figure 10 ZyXEL Utility: Profile .....	38
Figure 11 ZyXEL Utility: Add New Profile .....	38
Figure 12 ZyXEL Utility: Profile Security .....	39
Figure 13 ZyXEL Utility: Profile Encryption .....	39
Figure 14 Profile: Wireless Protocol Settings. ....	39
Figure 15 Profile: Confirm Save .....	40
Figure 16 Profile: Activate .....	40
Figure 17 Change Password Screen .....	42
Figure 18 Web Configurator Status Screen .....	44
Figure 19 Any IP Table .....	48
Figure 20 Summary: BW MGMT Monitor .....	49
Figure 21 Summary: DHCP Table .....	49
Figure 22 Summary: Packet Statistics .....	50
Figure 23 Summary: Wireless Association List .....	51
Figure 24 Select Wizard or Advanced Mode .....	55
Figure 25 Select a Language .....	56
Figure 26 Welcome to the Connection Wizard .....	56
Figure 27 Wizard Step 1: System Information .....	57
Figure 28 Wizard Step 2: Wireless LAN .....	58
Figure 29 Wizard Step 2: Basic (WEP) Security .....	59
Figure 30 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security .....	60
Figure 31 Wizard Step 3: ISP Parameters. ....	61
Figure 32 Wizard Step 3: Ethernet Connection .....	61
Figure 33 Wizard Step 3: PPPoE Connection .....	62
Figure 34 Wizard Step 3: PPTP Connection .....	63
Figure 35 Wizard Step 3: Your IP Address .....	64
Figure 36 Wizard Step 3: WAN IP and DNS Server Addresses .....	66
Figure 37 Wizard Step 3: WAN MAC Address .....	67
Figure 38 Wizard Step 4: Bandwidth Management .....	68

Figure 39 Connection Wizard Save .....	69
Figure 40 Connection Wizard Complete .....	69
Figure 41 Example of a Wireless Network .....	73
Figure 42 Wireless General .....	77
Figure 43 Wireless: No Security .....	78
Figure 44 Wireless: Static WEP Encryption .....	79
Figure 45 Wireless: WPA-PSK/WPA2-PSK .....	80
Figure 46 Wireless: WPA/WPA2 .....	81
Figure 47 MAC Address Filter .....	83
Figure 48 Wireless LAN Advanced .....	84
Figure 49 Wireless LAN QoS .....	86
Figure 50 Application Priority Configuration .....	87
Figure 51 Ethernet Encapsulation .....	90
Figure 52 PPPoE Encapsulation .....	93
Figure 53 PPTP Encapsulation .....	95
Figure 54 WAN > Advanced .....	97
Figure 55 Any IP Example .....	101
Figure 56 LAN IP .....	102
Figure 57 LAN IP Alias .....	103
Figure 58 Advanced LAN .....	104
Figure 59 DHCP Server General .....	105
Figure 60 DHCP Server Advanced .....	106
Figure 61 Client List .....	107
Figure 62 Multiple Servers Behind NAT Example .....	110
Figure 63 NAT General .....	110
Figure 64 NAT Application .....	112
Figure 65 Game List Example .....	114
Figure 66 Trigger Port Forwarding Process: Example .....	115
Figure 67 NAT Advanced .....	116
Figure 68 Dynamic DNS .....	120
Figure 69 Using IP Alias to Solve the Triangle Route Problem .....	123
Figure 70 General .....	123
Figure 71 Firewall Services .....	125
Figure 72 Content Filter: Filter .....	128
Figure 73 Content Filter: Schedule .....	129
Figure 74 Example of Static Routing Topology .....	133
Figure 75 IP Static Route .....	134
Figure 76 Static Route Setup .....	135
Figure 77 Subnet-based Bandwidth Management Example .....	138
Figure 78 Bandwidth Management: General .....	142
Figure 79 Bandwidth Management: Advanced .....	143
Figure 80 Bandwidth Management Rule Configuration: Pre-defined Service .....	145
Figure 81 Bandwidth Management Rule Configuration: User-defined Service .....	146

Figure 82 Bandwidth Management: Monitor .....	147
Figure 83 WWW Remote Management .....	150
Figure 84 Telnet Configuration on a TCP/IP Network .....	151
Figure 85 Telnet Remote Management .....	152
Figure 86 FTP Remote Management .....	152
Figure 87 DNS Remote Management .....	153
Figure 88 Configuring UPnP .....	156
Figure 89 Add/Remove Programs: Windows Setup: Communication .....	157
Figure 90 Add/Remove Programs: Windows Setup: Communication: Components .....	158
Figure 91 Network Connections .....	158
Figure 92 Windows Optional Networking Components Wizard .....	159
Figure 93 Networking Services .....	159
Figure 94 Network Connections .....	160
Figure 95 Internet Connection Properties .....	161
Figure 96 Internet Connection Properties: Advanced Settings .....	162
Figure 97 Internet Connection Properties: Advanced Settings: Add .....	162
Figure 98 System Tray Icon .....	163
Figure 99 Internet Connection Status .....	163
Figure 100 Network Connections .....	164
Figure 101 Network Connections: My Network Places .....	165
Figure 102 Network Connections: My Network Places: Properties: Example .....	165
Figure 103 System General .....	169
Figure 104 Time Setting .....	171
Figure 105 View Log .....	173
Figure 106 Log Settings .....	175
Figure 107 Maintenance Firmware Upload .....	187
Figure 108 Upload Warning .....	188
Figure 109 Network Temporarily Disconnected .....	188
Figure 110 Upload Error Message .....	188
Figure 111 Configuration .....	189
Figure 112 Configuration Restore Successful .....	190
Figure 113 Temporarily Disconnected .....	190
Figure 114 Configuration Restore Error .....	190
Figure 115 System Restart .....	191
Figure 116 Config Mode .....	193
Figure 117 Pop-up Blocker .....	207
Figure 118 Internet Options: Privacy .....	208
Figure 119 Internet Options: Privacy .....	209
Figure 120 Pop-up Blocker Settings .....	209
Figure 121 Internet Options: Security .....	210
Figure 122 Security Settings - Java Scripting .....	211
Figure 123 Security Settings - Java .....	211
Figure 124 Java (Sun) .....	212

Figure 125 Network Number and Host ID .....	214
Figure 126 Subnetting Example: Before Subnetting .....	216
Figure 127 Subnetting Example: After Subnetting .....	217
Figure 128 Wall-mounting Example .....	221
Figure 129 WIndows 95/98/Me: Network: Configuration .....	224
Figure 130 Windows 95/98/Me: TCP/IP Properties: IP Address .....	225
Figure 131 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	226
Figure 132 Windows XP: Start Menu .....	227
Figure 133 Windows XP: Control Panel .....	227
Figure 134 Windows XP: Control Panel: Network Connections: Properties .....	228
Figure 135 Windows XP: Local Area Connection Properties .....	228
Figure 136 Windows XP: Internet Protocol (TCP/IP) Properties .....	229
Figure 137 Windows XP: Advanced TCP/IP Properties .....	230
Figure 138 Windows XP: Internet Protocol (TCP/IP) Properties .....	231
Figure 139 Macintosh OS 8/9: Apple Menu .....	232
Figure 140 Macintosh OS 8/9: TCP/IP .....	232
Figure 141 Macintosh OS X: Apple Menu .....	233
Figure 142 Macintosh OS X: Network .....	234
Figure 143 Red Hat 9.0: KDE: Network Configuration: Devices .....	235
Figure 144 Red Hat 9.0: KDE: Ethernet Device: General .....	236
Figure 145 Red Hat 9.0: KDE: Network Configuration: DNS .....	236
Figure 146 Red Hat 9.0: KDE: Network Configuration: Activate .....	237
Figure 147 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .....	237
Figure 148 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .....	237
Figure 149 Red Hat 9.0: DNS Settings in resolv.conf .....	238
Figure 150 Red Hat 9.0: Restart Ethernet Card .....	238
Figure 151 Red Hat 9.0: Checking TCP/IP Properties .....	238
Figure 152 Peer-to-Peer Communication in an Ad-hoc Network .....	239
Figure 153 Basic Service Set .....	240
Figure 154 Infrastructure WLAN .....	241
Figure 155 RTS/CTS .....	242
Figure 156 WPA(2)-PSK Authentication .....	248
Figure 157 Displaying Log Categories Example .....	252
Figure 158 Displaying Log Parameters Example .....	252
Figure 159 Configuration Text File Format: Column Descriptions .....	261
Figure 160 Invalid Parameter Entered: Command Line Example .....	262
Figure 161 Valid Parameter Entered: Command Line Example .....	262
Figure 162 Internal SPTGEN FTP Download Example .....	263
Figure 163 Internal SPTGEN FTP Upload Example .....	263

# List of Tables

Table 1 Front Panel LEDs .....	31
Table 2 Status Screen Icon Key .....	44
Table 3 Web Configurator Status Screen .....	45
Table 4 Screens Summary .....	46
Table 5 Summary: DHCP Table .....	49
Table 6 Summary: Packet Statistics .....	50
Table 7 Summary: Wireless Association List .....	51
Table 8 Wizard Step 1: System Information .....	57
Table 9 Wizard Step 2: Wireless LAN .....	58
Table 10 Wizard Step 2: Basic (WEP) Security .....	59
Table 11 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security .....	60
Table 12 Wizard Step 3: ISP Parameters .....	61
Table 13 Wizard Step 3: PPPoE Connection .....	62
Table 14 Wizard Step 3: PPTP Connection .....	63
Table 15 Wizard Step 3: Your IP Address .....	64
Table 16 Private IP Address Ranges .....	64
Table 17 Wizard Step 3: WAN IP and DNS Server Addresses .....	66
Table 18 Example of Network Properties for LAN Servers with Fixed IP Addresses .....	67
Table 19 Wizard Step 3: WAN MAC Address .....	67
Table 20 Wizard Step 4: Bandwidth Management .....	68
Table 21 Types of Encryption for Each Type of Authentication .....	75
Table 22 WMM QoS Priorities .....	76
Table 23 Wireless General .....	77
Table 24 Wireless No Security .....	78
Table 25 Wireless: Static WEP Encryption .....	79
Table 26 Wireless: WPA-PSK/WPA2-PSK .....	80
Table 27 Wireless: WPA/WPA2 .....	82
Table 28 MAC Address Filter .....	83
Table 29 Wireless LAN Advanced .....	84
Table 30 Wireless LAN QoS .....	86
Table 31 Application Priority Configuration .....	87
Table 32 Ethernet Encapsulation .....	91
Table 33 PPPoE Encapsulation .....	93
Table 34 PPTP Encapsulation .....	96
Table 35 WAN > Advanced .....	98
Table 36 LAN IP .....	102
Table 37 LAN IP Alias .....	103
Table 38 Advanced LAN .....	104

Table 39 DHCP Server General .....	105
Table 40 DHCP Server Advanced .....	106
Table 41 Client List .....	108
Table 42 NAT General .....	111
Table 43 NAT Application .....	112
Table 44 NAT Advanced .....	116
Table 45 Dynamic DNS .....	120
Table 46 Firewall General .....	123
Table 47 Firewall Services .....	125
Table 48 Content Filter: Filter .....	128
Table 49 Content Filter: Schedule .....	130
Table 50 IP Static Route .....	134
Table 51 Static Route Setup .....	135
Table 52 Application and Subnet-based Bandwidth Management Example .....	138
Table 53 Bandwidth Management Priorities .....	138
Table 54 Media Bandwidth Management Setup: Services .....	139
Table 55 Commonly Used Services .....	140
Table 56 Bandwidth Management Priority with Default Classes .....	142
Table 57 Bandwidth Management: General .....	143
Table 58 Bandwidth Management: Advanced .....	144
Table 59 Bandwidth Management Rule Configuration: Pre-defined Service .....	145
Table 60 Bandwidth Management Rule Configuration: User-defined Service .....	146
Table 61 .....	149
Table 62 WWW Remote Management .....	151
Table 63 Telnet Remote Management .....	152
Table 64 FTP Remote Management .....	153
Table 65 DNS Remote Management .....	154
Table 66 Configuring UPnP .....	156
Table 67 System General .....	170
Table 68 Time Setting .....	171
Table 69 View Log .....	174
Table 70 Log Settings .....	175
Table 71 System Maintenance Logs .....	177
Table 72 System Error Logs .....	178
Table 73 Access Control Logs .....	178
Table 74 TCP Reset Logs .....	178
Table 75 Packet Filter Logs .....	179
Table 76 ICMP Logs .....	179
Table 77 CDR Logs .....	180
Table 78 PPP Logs .....	180
Table 79 UPnP Logs .....	180
Table 80 Content Filtering Logs .....	180
Table 81 Attack Logs .....	181



Table 82 PKI Logs .....	182
Table 83 802.1X Logs .....	183
Table 84 ACL Setting Notes .....	184
Table 85 ICMP Notes .....	184
Table 86 Syslog Logs .....	185
Table 87 RFC-2408 ISAKMP Payload Types .....	185
Table 88 Maintenance Firmware Upload .....	187
Table 89 Maintenance Restore Configuration .....	189
Table 90 Config Mode: Advanced Screens .....	193
Table 91 Hardware Features .....	203
Table 92 Firmware Features .....	203
Table 93 Subnet Mask - Identifying Network Number .....	214
Table 94 Subnet Masks .....	215
Table 95 Maximum Host Numbers .....	215
Table 96 Alternative Subnet Mask Notation .....	215
Table 97 Subnet 1 .....	217
Table 98 Subnet 2 .....	218
Table 99 Subnet 3 .....	218
Table 100 Subnet 4 .....	218
Table 101 Eight Subnets .....	218
Table 102 24-bit Network Number Subnet Planning .....	219
Table 103 16-bit Network Number Subnet Planning .....	219
Table 104 IEEE 802.11g .....	243
Table 105 Comparison of EAP Authentication Types .....	246
Table 106 Wireless Security Relational Matrix .....	249
Table 107 NetBIOS Filter Default Settings .....	256
Table 108 Examples of Services .....	257
Table 109 Abbreviations Used in the Example Internal SPTGEN Screens Table .....	264
Table 110 Menu 1 General Setup .....	264
Table 111 Menu 3 .....	264
Table 112 Menu 4 Internet Access Setup .....	267
Table 113 Menu 12 .....	269
Table 114 Menu 15 SUA Server Setup .....	269
Table 115 Menu 21.1 Filter Set #1 .....	271
Table 116 Menu 21.1 Filter Set #2, .....	272
Table 117 Menu 23 System Menus .....	274
Table 118 Menu 24.11 Remote Management Control .....	275
Table 119 Command Examples .....	276



---

# PART I

# Introduction

---

Getting to Know Your ZyXEL Device (29)

Wireless Tutorial (33)

Introducing the Web Configurator (41)



# Getting to Know Your ZyXEL Device

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

## 1.1 ZyXEL Device Overview

The ZyXEL Device is the ideal secure wireless firewall router for all data passing between the Internet and your Local Area Network.

You can configure firewall and/or content filtering for secure Internet access. You can also use media bandwidth management to efficiently manage traffic on your network. The Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

The ZyXEL Device has an embedded mini-PCI module for 802.11g Wireless LAN connectivity. The ZyXEL Device supports the IEEE 802.11b and g standards, so that either IEEE 802.11b or IEEE 802.11g compatible clients can wirelessly access the ZyXEL Device or the wired network behind it. The ZyXEL Device allows you to access wireless networks at speeds of up to 108Mbps (with the Super G function enabled)



---

Only use firmware for your ZyXEL Device's specific model.

---

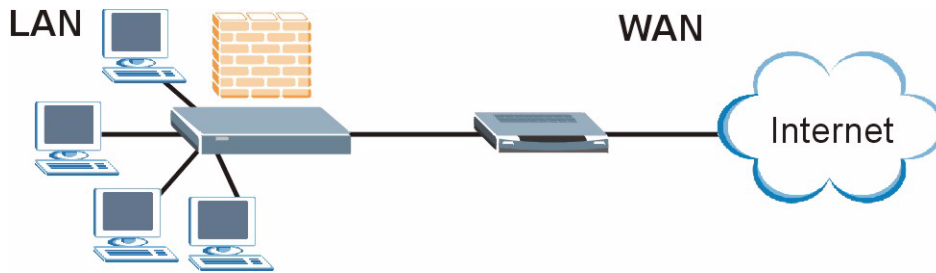
## 1.2 Applications for the ZyXEL Device

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

### 1.2.1 Secure Broadband Internet Access

You can connect a cable modem, DSL or wireless modem to the ZyXEL Device for broadband Internet access via an Ethernet or a wireless port on the modem. The ZyXEL Device guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

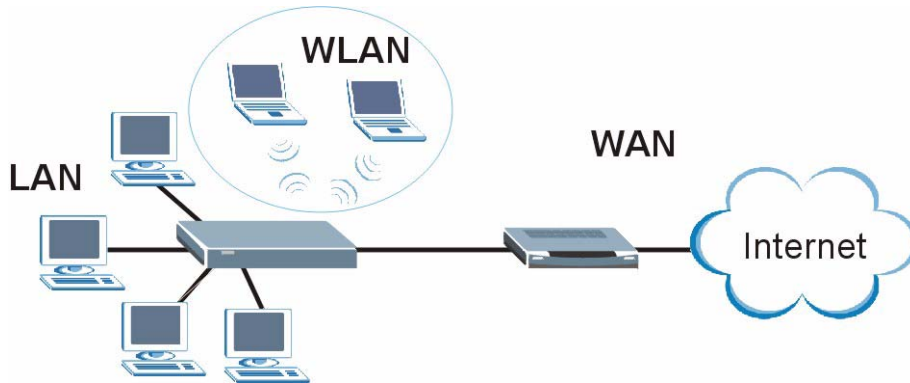
**Figure 1** Secure Internet Access via Cable, DSL or Wireless Modem



### 1.2.1.1 Wireless LAN Application

Add a wireless LAN to your existing network without expensive network cables. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network.

**Figure 2** WLAN Application Example



## 1.3 Ways to Manage the ZyXEL Device

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

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

## 1.4 Good Habits for Managing the ZyXEL Device

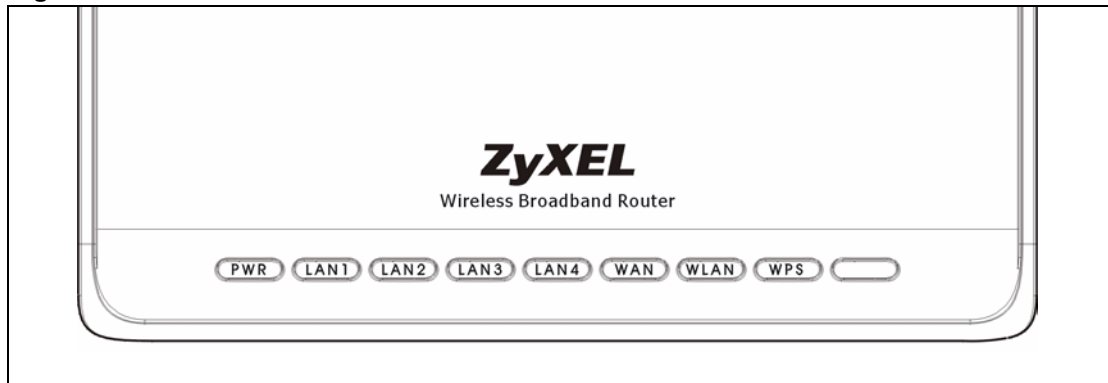
Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- 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.

## 1.5 LEDs

**Figure 3** Front Panel



The following table describes the LEDs.

**Table 1** Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
<b>PWR</b>	Green	On	The ZyXEL Device is receiving power and functioning properly.
	None	Off	The ZyXEL Device is not receiving power.
<b>LAN 1-4</b>	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.
None	Off	The LAN is not connected.	
<b>WAN</b>	Green	On	The ZyXEL Device has a successful 10Mb WAN 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.
	None	Off	The WAN connection is not ready, or has failed.

**Table 1** Front Panel LEDs (continued)

<b>LED</b>	<b>COLOR</b>	<b>STATUS</b>	<b>DESCRIPTION</b>
<b>WLAN</b>	Green	On	The ZyXEL Device is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The ZyXEL Device is sending/receiving data through the wireless LAN.
	None	Off	The wireless LAN is not ready or has failed.
<b>WPS</b>			This LED is reserved for future firmware release.



# Wireless Tutorial

This chapter gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through an AP wirelessly.

## 2.1 Example Parameters

<b>SSID</b>	SSID_Example3
<b>Channel</b>	6
<b>Security</b>	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
<b>802.11 mode</b>	IEEE 802.11b/g

An access point (AP) or wireless router is referred to as an “AP” and a computer with a wireless network card or USB/PCI adapter is referred to as a “wireless client” here.

We use the M-302 utility screens as an example for the wireless client. The screens may vary for different models.

## 2.2 Configuring the AP

Flow the steps below to configure the wireless settings on your AP.

- 1 Open the **Wireless LAN > General** screen in the AP’s web configurator.

**Figure 4** AP: Wireless LAN > General

**Wireless Setup**

Enable Wireless LAN

Name(SSID)

Hide SSID

Channel Selection

Operating Channel

**Security**

Security Mode

Pre-Shared Key

ReAuthentication Timer  (In Seconds)

Idle Timeout  (In Seconds)

Group Key Update Timer  (In Seconds)

- 2 Make sure the **Enable Wireless LAN** check box is selected.
- 3 Enter **SSID\_Example3** as the SSID and select a channel.
- 4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.
- 5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 5 AP: Status

The screenshot displays the ZyXEL NBG-310SH AP Status page. The left sidebar shows navigation options: Network (Wireless LAN, WAN, LAN, DHCP Server, NAT, DDNS), Security (Firewall, Content Filter), Management (Static Route, Bandwidth MGMT, Remote MGMT, UPnP), and Maintenance (System, Logs, Tools). The main content area is divided into several sections:

- Device Information:** System Name: NBG-334SH, Firmware Version: V3.60(AMG.0)b1 | 11/23/2006.
  - WAN Information: MAC Address: 00:13:49:00:00:02, IP Address: -, IP Subnet Mask: -, DHCP: -
  - LAN Information: MAC Address: 00:13:49:00:00:01, IP Address: 172.23.37.210, IP Subnet Mask: 255.255.255.0, DHCP: -
  - WLAN Information (circled in red): MAC Address: 00:13:49:a9:b1:28, Name(SSID): SSID\_Example3, Channel: 6, Operating Channel: 6, Security Mode: WPA-PSK, 802.11 Mode: 802.11b/g
- System Status:** System Up Time: 2:24:33, Current Date/Time: 2000-1-1/2:24:30. System Resource: CPU Usage: 3.31%, Memory Usage: 40%. System Setting: Firewall: Enabled, Bandwidth Management: Disabled, UPnP: Enabled.
- Interface Status:** A table showing interface status:
 

Interface	Status	Rate
WAN	Down	N/A
LAN	Up	100M/Full
WLAN	Up	54M
- Summary:** Includes links for Any IP Table, BW MGMT Monitor, DHCP Table, Packet Statistics, and WLAN Station Status (circled in red).

- 6 Click the **WLAN Station Status** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

Figure 6 AP: Status: WLAN Station Status

The screenshot shows the WLAN Station Status page with an Association List table:

#	MAC Address	Association Time
001	00:13:49:63:3f:5e	00:18:23 2000/01/01

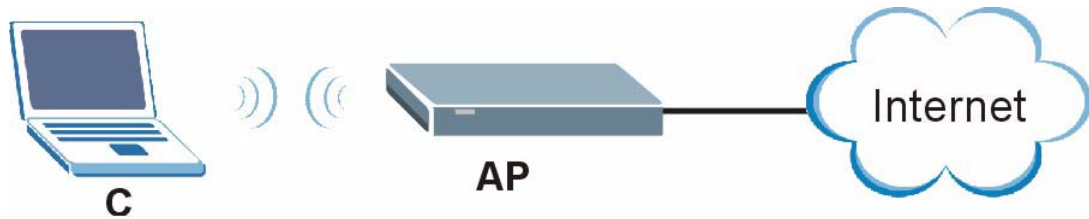
Below the table is a Refresh button.

## 2.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

### 2.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



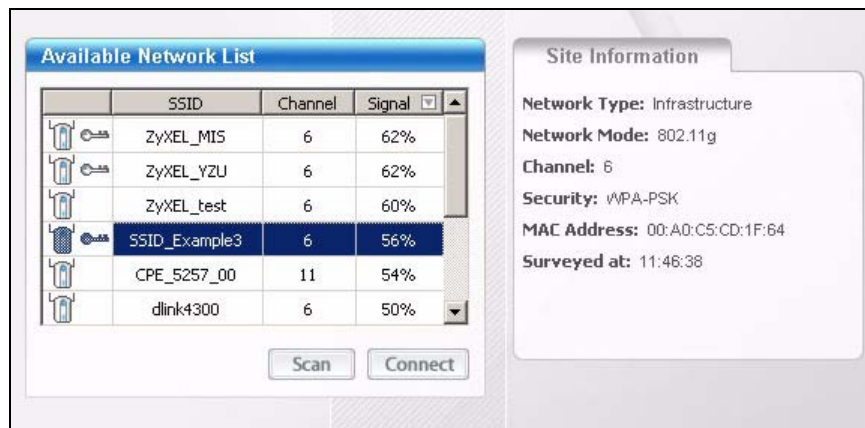
There are three ways to connect the client to an access point.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is “SSID\_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”.

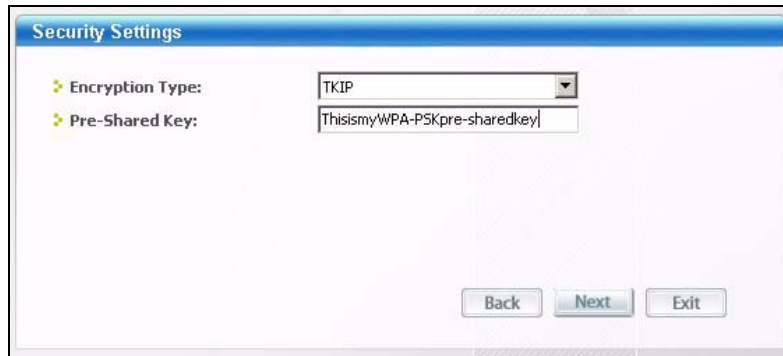
After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

- 1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

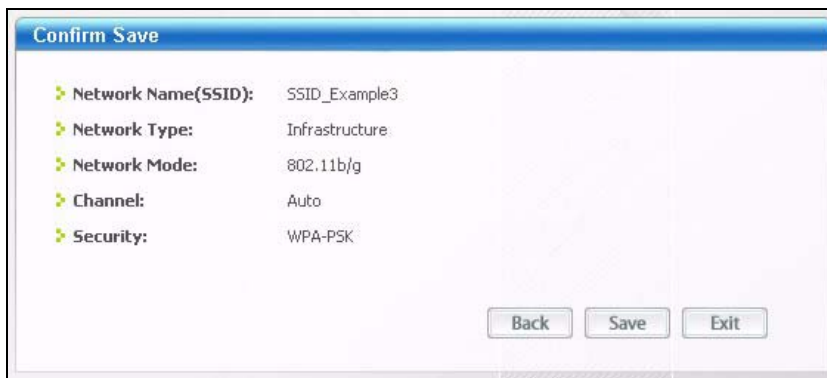


- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.
- 3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

**Figure 7** ZyXEL Utility: Security Settings

- 4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

**Figure 8** ZyXEL Utility: Confirm Save

- 5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

**Figure 9** ZyXEL Utility: Link Info

- 6 Open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

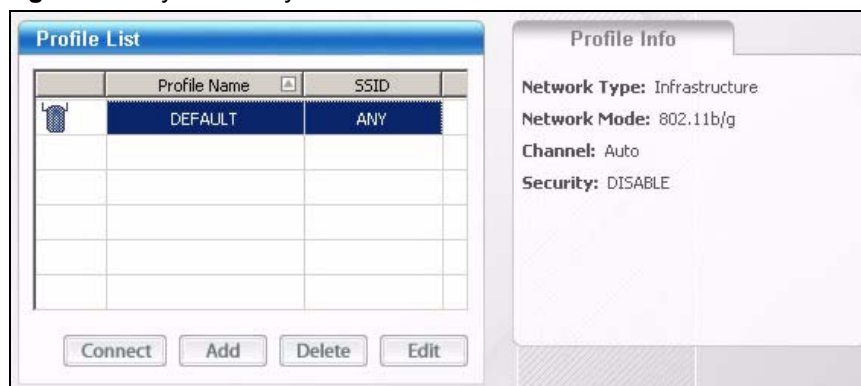
## 2.3.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the wireless client. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is “SSID\_Example3”, the profile name is “PN\_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”. You have chosen the profile name “PN\_Example3”.

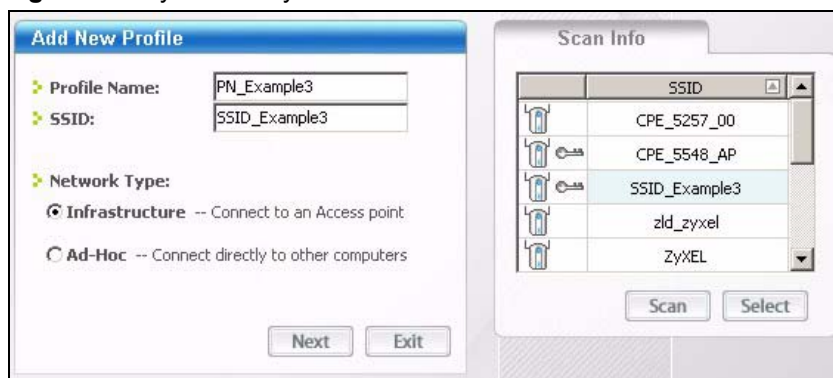
- 1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

**Figure 10** ZyXEL Utility: Profile



- 2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. Click on **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

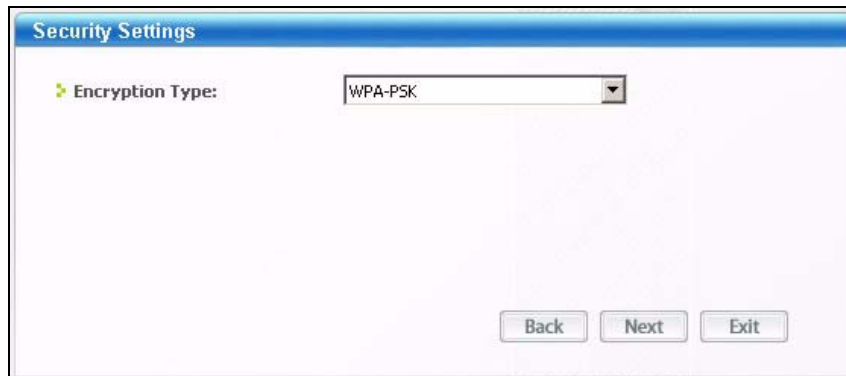
**Figure 11** ZyXEL Utility: Add New Profile



- 3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

- 4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

**Figure 12** ZyXEL Utility: Profile Security



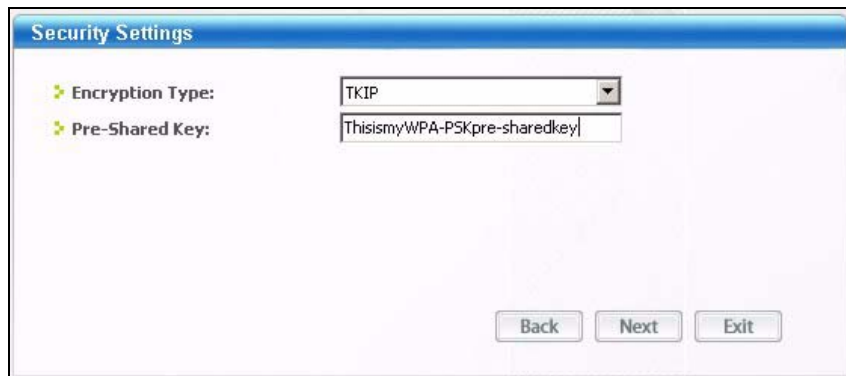
Security Settings

Encryption Type: WPA-PSK

Back Next Exit

- 5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.

**Figure 13** ZyXEL Utility: Profile Encryption



Security Settings

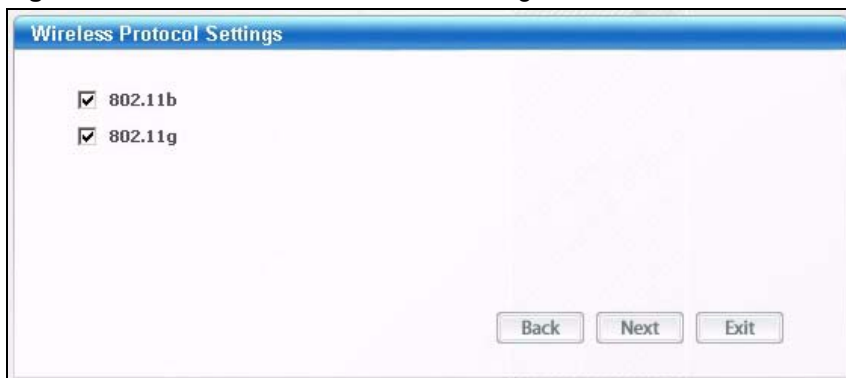
Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

Back Next Exit

- 6 In the next screen, leave both boxes checked.

**Figure 14** Profile: Wireless Protocol Settings.



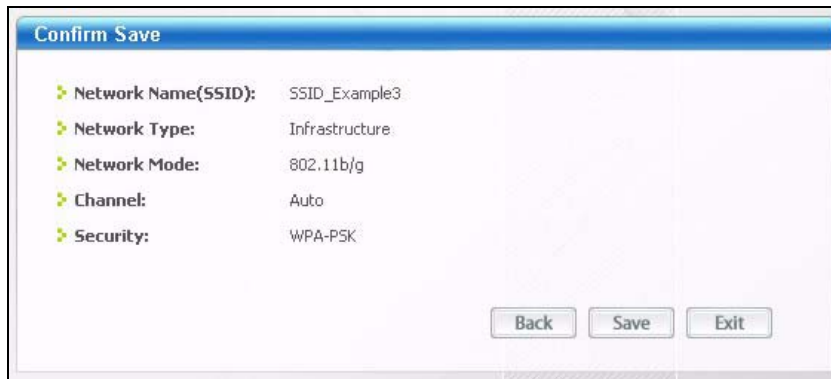
Wireless Protocol Settings

802.11b

802.11g

Back Next Exit

- 7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.

**Figure 15** Profile: Confirm Save

- 8** Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.



Only one profile can be activated and used at any given time.

**Figure 16** Profile: Activate

- 9** When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.
- 10** Open your Internet browser, enter <http://www.zyxel.com> or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.
- 11** If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.



# Introducing the Web Configurator

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

## 3.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy setup and management of the ZyXEL Device 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).

Refer to the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

## 3.2 Accessing the Web Configurator

- 1 Make sure your ZyXEL Device hardware is properly connected and prepare your computer or computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 17 Change Password Screen

**ZyXEL**

Please enter a new 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.

The administrator password should must be between 1 - 30 characters.

**New Password:**

**Retype to Confirm:**

Apply Ignore



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.

- 6 Select the setup mode you want to use.
  - Click **Go to Wizard Setup** to use the Configuration Wizard for basic Internet and Wireless setup.
  - Click **Go to Basic Setup** if you want to view and configure basic settings that are not part of the wizard setup. Not all Web Configurator screens are available in this mode.
  - Click **Go to Advanced Setup** to view and configure all the ZyXEL Device's settings.

**ZyXEL**

Please select Wizard, Basic, 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.

Use Basic mode if you need to make basic configuration changes.

Use Advanced mode if you need access to more advanced features.

[Go to Wizard setup \(You have previously completed Wizard setup\)](#)

[Go to Basic setup](#)

[Go to Advanced setup](#)

Exit

## 3.3 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 saved, and the password will be reset to “1234”.

### 3.3.1 Procedure to Use the Reset Button

- 1 Make sure the **PWR** LED is on.
- 2 Press the **RESET** button for ten seconds or until the **PWR** LED begins to blink and then release it. When the **PWR** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts.

## 3.4 Navigating the Web Configurator

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

### 3.4.1 The Status Screen

The following screen displays when you log into the ZyXEL Device.



---

Not all fields are available when you select **Basic** mode (see [Section 3.2 on page 41](#)). See the **Configuration Mode** field in the **System Status** box to check whether you are in **Basic** or **Advanced** mode. Use the **Config Mode > General** screen to change between modes.

---

Figure 18 Web Configurator Status Screen



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

Table 2 Status Screen Icon Key

ICON	DESCRIPTION
	Select a language from the drop-down list box to have the web configurator display in that language.
	Click this icon to open a web help page relevant to the screen you are currently configuring.
	Click this icon to open the setup wizard.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the web configurator.
	Select a number of seconds or <b>None</b> 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.
	Click this button to refresh the status screen statistics.

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

**Table 3** Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the <b>System Name</b> you enter in the <b>Maintenance &gt; System &gt; General</b> screen. It is for identification purposes.
Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- DHCP	This shows the WAN port's DHCP role - <b>Client</b> or <b>None</b> .
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - <b>Server, Relay</b> or <b>None</b> .
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Name (SSID)	This shows a descriptive name used to identify the ZyXEL Device in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the ZyXEL Device is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the ZyXEL Device is using.
- 802.11 Mode	This shows the wireless standard.
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 Resource	
- CPU Usage	This displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management).
- Memory Usage	This shows what percentage of the heap memory the ZyXEL Device is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall.
System Setting	
- Firewall	This shows whether the firewall is active or not.
- Bandwidth Management	This shows whether the bandwidth management is active or not.
- UPnP	This shows whether UPnP is active or not.

**Table 3** Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
- Configuration Mode	This shows whether the advanced screens of each feature are turned on ( <b>Advanced</b> ) or not ( <b>Basic</b> ).
Interface Status	
Interface	This displays the ZyXEL Device port types. The port types are: <b>WAN</b> , <b>LAN</b> and <b>WLAN</b> .
Status	For the LAN and WAN ports, this field displays <b>Down</b> (line is down) or <b>Up</b> (line is up or connected). For the WLAN, it displays <b>Up</b> when the WLAN is enabled or <b>Down</b> when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or <b>N/A</b> when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays <b>N/A</b> when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and <b>N/A</b> when the WLAN is disabled.
Summary	
Any IP Table	Use this screen to view details of IP addresses assigned to devices not in the same subnet as the ZyXEL Device.
BW MGMT Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
DHCP Table	Use this screen to view current DHCP client information.
Packet Statistics	Use this screen to view port status and packet specific statistics.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the ZyXEL Device.

### 3.4.2 Navigation Panel

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

The following table describes the sub-menus.

**Table 4** Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the ZyXEL Device's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the ZyXEL Device to block access to devices or block the devices from accessing the ZyXEL Device.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.

**Table 4** Screens Summary

LINK	TAB	FUNCTION
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	Advanced	Use this screen to configure other advanced properties.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Advanced	Use this screen to enable other advanced properties.
DHCP Server	General	Use this screen to enable the ZyXEL Device's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	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).
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the ZyXEL Device.
	Advanced	Use this screen to change your ZyXEL Device's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Filter	Use this screen to block certain web features and 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.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes.
Bandwidth MGMT	General	Use this screen to enable bandwidth management.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
	Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use 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.
	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.

**Table 4** Screens Summary

LINK	TAB	FUNCTION
UPnP	General	Use this screen to enable UPnP on the ZyXEL Device.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	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.
Config Mode	General	This screen allows you to display or hide the advanced screens or features.

### 3.5 Summary: Any IP Table

This screen displays the IP address of each computer that is using the ZyXEL Device via the any IP feature. Any IP allows computers to access the Internet through the ZyXEL Device without changing their network settings when NAT is enabled. To access this screen, open the **Status** screen (see [Section 3.4.1 on page 43](#)), and click **(Details...)** next to **Any IP Table**.

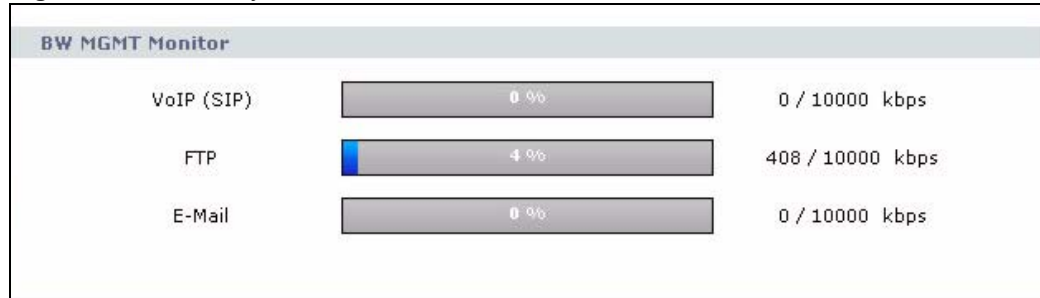
**Figure 19** Any IP Table


Any IP TABLE		
#	IP Address	MAC Address
Refresh		

#### 3.5.1 Summary: Bandwidth Management Monitor

Select the **BW MGMT Monitor (Details...)** hyperlink in **Status** screen. View the bandwidth usage of the WAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.



**Figure 20** Summary: BW MGMT Monitor

### 3.5.2 Summary: DHCP Table

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

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

**Figure 21** Summary: DHCP Table

DHCP Table			
#	IP Address	Host Name	MAC Address
1	192.168.1.33	1147	00:00:8d:48:00:00

Refresh

The following table describes the labels in this screen.

**Table 5** Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the <b>Host Name</b> field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click <b>Refresh</b> to renew the screen.

### 3.5.3 Summary: Packet Statistics

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

**Figure 22** Summary: Packet Statistics

Packet Statistics							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Idle	210266	156607	0	0	448	0:00:00
LAN	100M/Full	247620	61040	0	0	0	8:01:43
WLAN	54M	1138	0	0	0	0	8:01:43

**System Up Time : 8:01:49**

Poll Interval(s) :  sec

The following table describes the labels in this screen.

**Table 6** Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the ZyXEL Device's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or <b>Down</b> when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays <b>Down</b> when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and <b>Down</b> when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyXEL Device has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click <b>Stop</b> to stop refreshing statistics, click <b>Stop</b> .

### 3.5.4 Summary: Wireless Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the ZyXEL Device in the **Association List** screen.

**Figure 23** Summary: Wireless Association List

Association List		
#	MAC Address	Association Time
001	00:0e:35:96:6d:6a	01:38:47 2000/01/01

Refresh

The following table describes the labels in this screen.

**Table 7** Summary: Wireless Association List

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



---

# PART II

## Wizard

---

Connection Wizard (55)



# Connection Wizard

This chapter provides information on the wizard setup screens in the web configurator.

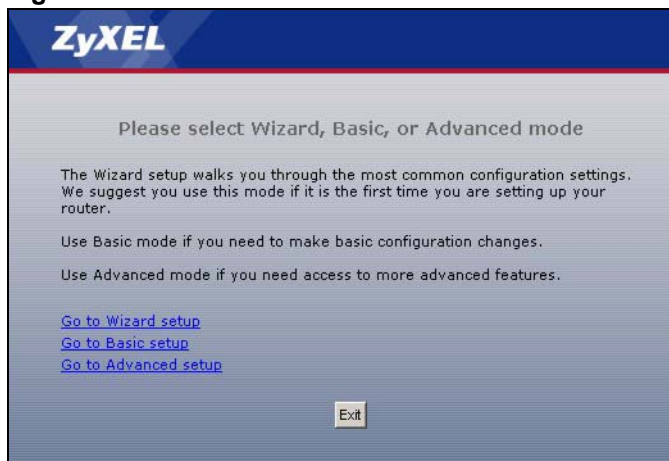
## 4.1 Wizard Setup

The web configurator's wizard setup helps you configure your device to access the Internet. Refer to your ISP (Internet Service Provider) checklist in the Quick Start Guide to know what to enter in each field. Leave a field blank if you don't have that information.

- 1 After you access the ZyXEL Device web configurator, click the **Go to Wizard setup** hyperlink.

You can click the **Go to Basic setup** or **Go to Advanced setup** hyperlink to skip this wizard setup and configure basic or advanced features accordingly.

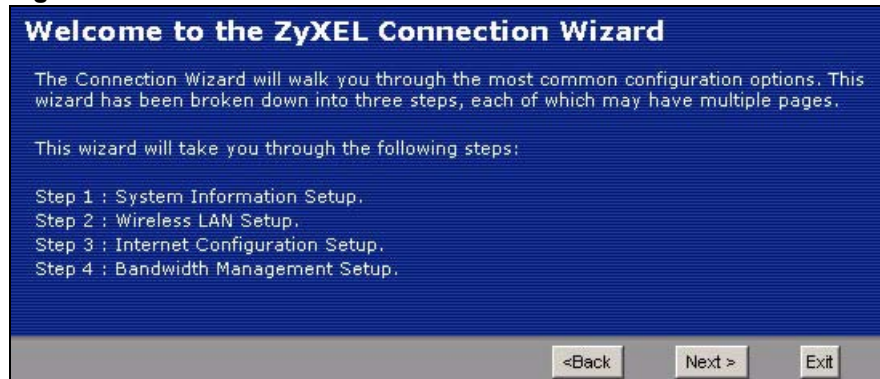
**Figure 24** Select Wizard or Advanced Mode



- 2 Choose your language from the drop-down list box.
- 3 Click the **Next** button to proceed to the next screen.

**Figure 25** Select a Language

4 Read the on-screen information and click **Next**.

**Figure 26** Welcome to the Connection Wizard

## 4.2 Connection Wizard: STEP 1: System Information

**System Information** contains administrative and system-related information.

### 4.2.1 System Name

**System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start, Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.



## 4.2.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyXEL Device via DHCP.

Click **Next** to configure the ZyXEL Device for Internet access.

**Figure 27** Wizard Step 1: System Information

The following table describes the labels in this screen.

**Table 8** Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the ZyXEL Device in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

## 4.3 Connection Wizard: STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

**Figure 28** Wizard Step 2: Wireless LAN

The following table describes the labels in this screen.

**Table 9** Wizard Step 2: Wireless LAN

LABEL	DESCRIPTION
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.
Security	Select a <b>Security</b> level from the drop-down list box. Choose <b>Auto</b> to have the ZyXEL Device generate a pre-shared key automatically. A screen pops up displaying the generated pre-shared key after you click <b>Next</b> . Click <b>OK</b> to continue. Choose <b>None</b> to have no wireless LAN security configured. If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to <a href="#">Section 4.4 on page 60</a> . Choose <b>Basic (WEP)</b> security if you want to configure WEP Encryption parameters. If you choose this option, go directly to <a href="#">Section 4.3.1 on page 59</a> . Choose <b>Extend (WPA-PSK or WPA2-PSK)</b> security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK or WPA2-PSK respectively. If you choose this option, skip directly to <a href="#">Section 4.3.2 on page 60</a> .
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel that is not used by any nearby devices.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.



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) or WPA2-PSK (if WPA2-PSK is enabled) for wireless communication.

### 4.3.1 Basic (WEP) Security

Choose **Basic (WEP)** to setup WEP Encryption parameters.

**Figure 29** Wizard Step 2: Basic (WEP) Security

The following table describes the labels in this screen.

**Table 10** Wizard Step 2: Basic (WEP) Security

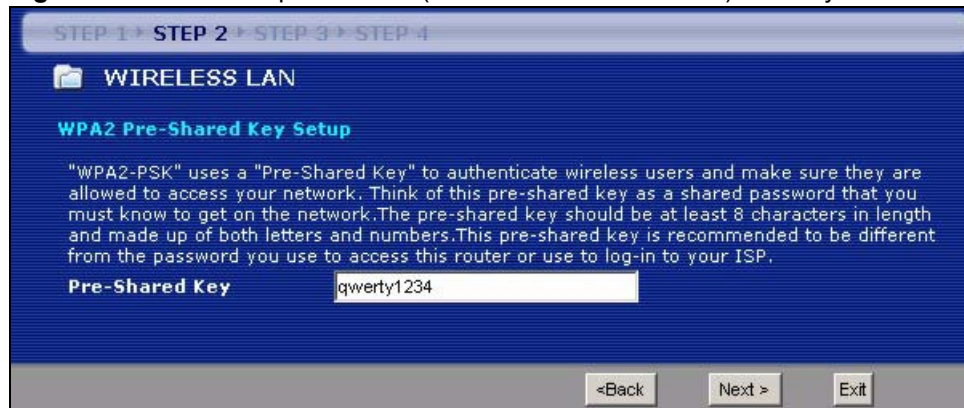
LABEL	DESCRIPTION
Passphrase	Type a Passphrase (up to 32 printable characters) and click <b>Generate</b> . The ZyXEL Device automatically generates a WEP key.
WEP Encryption	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you chose <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Back	Click <b>Back</b> to display the previous screen.

**Table 10** Wizard Step 2: Basic (WEP) Security

LABEL	DESCRIPTION
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

### 4.3.2 Extend (WPA-PSK or WPA2-PSK) Security

Choose **Extend (WPA-PSK)** or **Extend (WPA2-PSK)** security in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

**Figure 30** Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

The following table describes the labels in this screen.

**Table 11** Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

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

## 4.4 Connection Wizard: STEP 3: Internet Configuration

The ZyXEL Device offers three Internet connection types. They are **Ethernet**, **PPP over Ethernet** or **PPTP**. The wizard attempts to detect which WAN connection type you are using. If the wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

This wizard screen varies according to the connection type that you select.

**Figure 31** Wizard Step 3: ISP Parameters.

The following table describes the labels in this screen,

**Table 12** Wizard Step 3: ISP Parameters

CONNECTION TYPE	DESCRIPTION
Ethernet	Select the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet.
PPPoE	Select the <b>PPP over Ethernet</b> option for a dial-up connection. If your ISP gave you a an IP address and/or subnet mask, then select <b>PPTP</b> .
PPTP	Select the <b>PPTP</b> option for a dial-up connection.

#### 4.4.1 Ethernet Connection

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

**Figure 32** Wizard Step 3: Ethernet Connection

#### 4.4.2 PPPoE Connection

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

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

One of the benefits of PPPoE is the ability to let end users 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 specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's 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 LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.

**Figure 33** Wizard Step 3: PPPoE Connection

The following table describes the labels in this screen.

**Table 13** Wizard Step 3: PPPoE Connection

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Connection Type	Select the <b>PPP over Ethernet</b> option for a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

### 4.4.3 PPTP Connection

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

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

Refer to the appendix for more information on PPTP.



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

**Figure 34** Wizard Step 3: PPTP Connection

The following table describes the fields in this screen

**Table 14** Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select <b>PPTP</b> from the drop-down list box. To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this radio button, provided by your ISP to give the ZyXEL Device a fixed, unique IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Back	Click <b>Back</b> to return to the previous screen.

**Table 14** Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
Next	Click <b>Next</b> to continue.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

#### 4.4.4 Your IP Address

The following wizard screen allows you to assign a fixed IP address or give the ZyXEL Device an automatically assigned IP address depending on your ISP.

**Figure 35** Wizard Step 3: Your IP Address

The following table describes the labels in this screen

**Table 15** Wizard Step 3: Your IP Address

LABEL	DESCRIPTION
Get automatically from your ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection. If you choose this option, skip directly to section <a href="#">4.4.9</a> .
Use fixed IP address provided by your ISP	Select this option if you were given IP address and/or DNS server settings by the ISP. The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

#### 4.4.5 WAN IP Address Assignment

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

**Table 16** Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255



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



---

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

---

#### 4.4.6 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. 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.

#### 4.4.7 DNS Server Address Assignment

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

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

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **Wizard** and/or **WAN > Internet Connection** screen.

- If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

#### 4.4.8 WAN IP and DNS Server Address Assignment

The following wizard screen allows you to assign a fixed WAN IP address and DNS server addresses.

**Figure 36** Wizard Step 3: WAN IP and DNS Server Addresses

The screenshot shows a wizard interface with a blue background. At the top, it says 'STEP 1 > STEP 2 > STEP 3 > STEP 4'. Below that is a folder icon and the text 'Internet Configuration'. Underneath is the section 'WAN IP Address Assignment' with three input fields: 'My WAN IP Address' (172.23.23.49), 'My WAN IP Subnet Mask' (255.255.255.0), and 'Gateway IP Address' (0.0.0.0). Below that is the section 'DNS Server Address Assignment' with three input fields: 'First DNS Server' (172.23.5.1), 'Second DNS Server' (172.23.5.2), and 'Third DNS Server' (0.0.0.0). At the bottom right, there are three buttons: '<Back', 'Next >', and 'Exit'.

The following table describes the labels in this screen

**Table 17** Wizard Step 3: WAN IP and DNS Server Addresses

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Enter your WAN IP address in this field. The WAN IP address should be in the same subnet as your DSL/Cable modem or router.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
System DNS Server Address Assignment (if applicable) 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 computer before you can access it. The ZyXEL Device uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.	
First DNS Server Second DNS Server Third DNS Server	Enter the DNS server's IP address in the fields provided. If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

## 4.4.9 WAN MAC Address

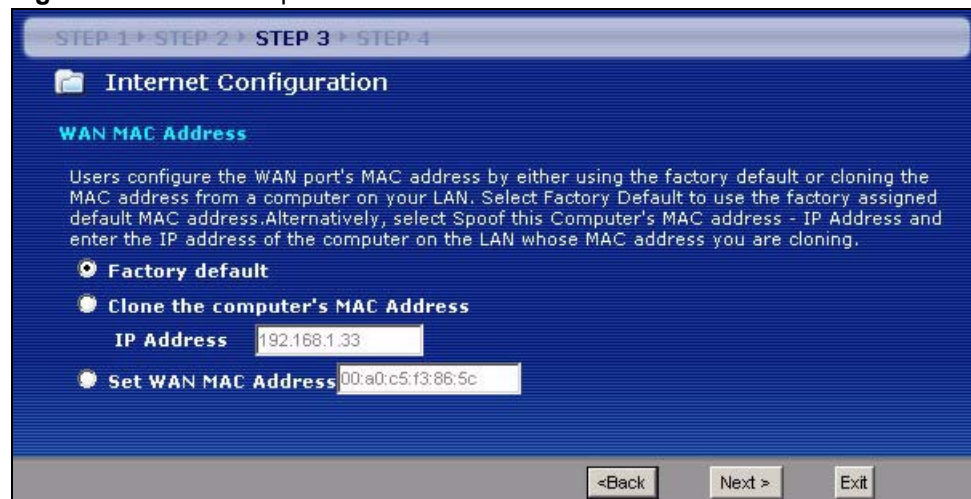
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

**Table 18** Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(ZyXEL Device LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.

**Figure 37** Wizard Step 3: WAN MAC Address



The following table describes the fields in this screen.

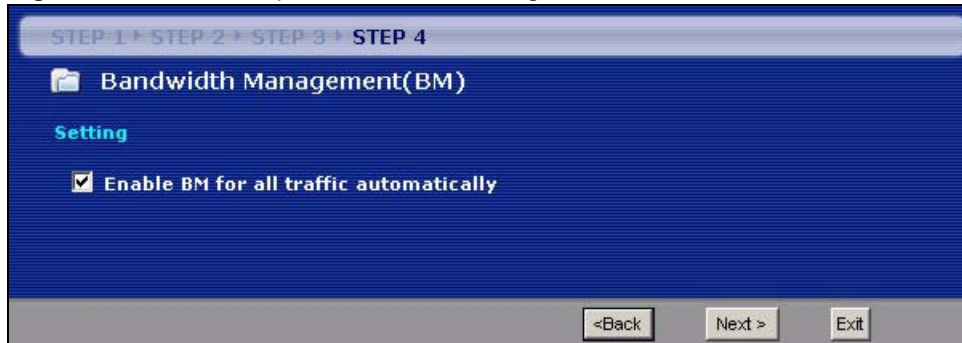
**Table 19** Wizard Step 3: WAN MAC Address

LABEL	DESCRIPTION
Factory Default	Select <b>Factory Default</b> to use the factory assigned default MAC address.
Clone the computer's MAC address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

## 4.5 Connection Wizard: STEP 4: Bandwidth management

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

**Figure 38** Wizard Step 4: Bandwidth Management



The following fields describe the label in this screen.

**Table 20** Wizard Step 4: Bandwidth Management

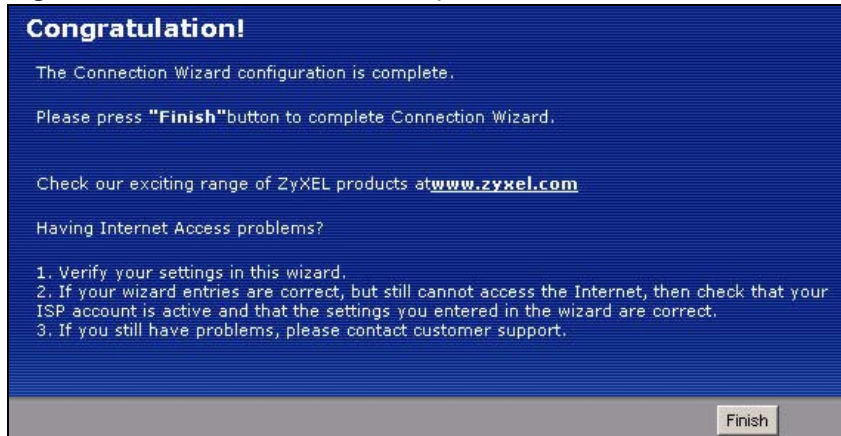
LABEL	DESCRIPTION
Enable BM for all traffic automatically	Select the check box to have the ZyXEL Device apply bandwidth management to traffic going out through the ZyXEL Device's WAN, LAN or WLAN port. Bandwidth is allocated according to the traffic type automatically. Real-time packets, such as VoIP traffic always get higher priority.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

## 4.6 Connection Wizard Complete

Click **Apply** to save your configuration.

**Figure 39** Connection Wizard Save

Follow the on-screen instructions and click **Finish** to complete the wizard setup.

**Figure 40** Connection Wizard Complete

Well done! You have successfully set up your ZyXEL Device to operate on your network and access the Internet.



---

# PART III

## Advanced

---

Wireless LAN (73)  
WAN (89)  
LAN (99)  
DHCP Server (105)  
Network Address Translation (NAT) (109)  
Dynamic DNS (119)  
Firewall (121)  
Content Filtering (127)  
Static Route Screens (133)  
Bandwidth Management (137)  
Remote Management Screens (149)  
Universal Plug-and-Play (UPnP) (155)





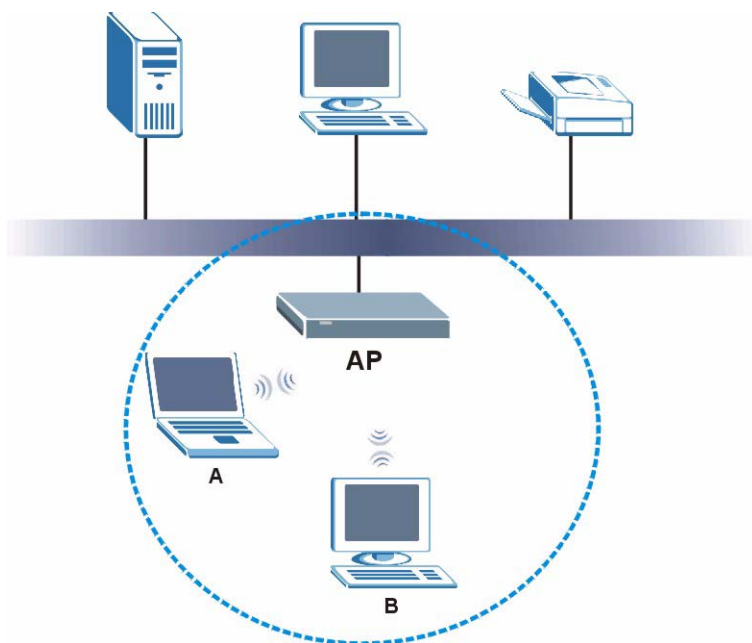
# Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. See the appendices for more detailed information about wireless networks.

## 5.1 Wireless Network Overview

The following figure provides an example of a wireless network.

**Figure 41** Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID. The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels. Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.  
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## 5.2 Wireless Security Overview

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

### 5.2.1 SSID

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

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

### 5.2.2 MAC Address Filter

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

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

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

### 5.2.3 User Authentication

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

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

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

---

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.  
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

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

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


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

## 5.2.4 Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See [Section 5.2.3 on page 74](#) for information about this.)

**Table 21** Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
<b>Weakest</b>  <b>Strongest</b>	No Security	WPA
	Static WEP	
	WPA-PSK	
	WPA2-PSK	WPA2

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

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



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

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

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

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

## 5.3 Quality of Service

This section discusses the Quality of Service (QoS) features available on the ZyXEL Device.

### 5.3.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to delivery requirements. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The ZyXEL Device uses WMM QoS to prioritize traffic streams according to the IEEE 802.1p tag or DSCP information in each packet's header. The ZyXEL Device automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency (delay) and jitter (variations in delay).

#### 5.3.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the ZyXEL Device uses.

**Table 22** WMM QoS Priorities

PRIORITY LEVEL	DESCRIPTION
voice (WMM_VOICE)	Typically used for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality.
video (WMM_VIDEO)	Typically used for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.
best effort (WMM_BEST_EFFORT)	Typically used for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
background (WMM_BACKGROUND)	This is typically used for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements.

## 5.4 General Wireless LAN Screen



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

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

**Figure 42** Wireless General

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

**Table 23** Wireless General

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set Identity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on whether you are using A or B/G frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels.
Operating Channel	This displays the channel the ZyXEL Device is currently using.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

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

## 5.4.1 No Security

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



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

**Figure 43** Wireless: No Security

The following table describes the labels in this screen.

**Table 24** Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose <b>No Security</b> from the drop-down list box.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 5.4.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

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

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

Figure 44 Wireless: Static WEP Encryption

**Wireless Setup**

Enable Wireless LAN

Name(SSID)

Hide SSID

Channel Selection

Operating Channel

**Security**

Security Mode

Passphrase

WEP Encryption

Authentication Method

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

ASCII  Hex

Key 1

Key 2

Key 3

Key 4

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

Table 25 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Passphrase	Enter a passphrase (password phrase) of up to 32 printable characters and click <b>Generate</b> . The ZyXEL Device automatically generates four different WEP keys and displays them in the <b>Key</b> fields below.
WEP Encryption	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.
Authentication Method	This field is activated when you select <b>64-bit WEP</b> or <b>128-bit WEP</b> in the <b>WEP Encryption</b> field. Select <b>Auto</b> , <b>Open System</b> or <b>Shared Key</b> from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you chose <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

### 5.4.3 WPA-PSK/WPA2-PSK

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

**Figure 45** Wireless: WPA-PSK/WPA2-PSK

The screenshot shows the 'General' tab of the 'Wireless Setup' configuration page. The 'Wireless Setup' section includes:
 

- Enable Wireless LAN
- Name(SSID): ZyXEL
- Hide SSID
- Channel Selection: Channel-01 2412MHz
- Operating Channel: Channel-006

 The 'Security' section includes:
 

- Security Mode: WPA2-PSK
- WPA Compatible
- Pre-Shared Key: [Empty text box]
- ReAuthentication Timer: 1800 (In Seconds)
- Idle Timeout: 3600 (In Seconds)
- Group Key Update Timer: 1800 (In Seconds)

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

The following table describes the labels in this screen.

**Table 26** Wireless: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select <b>WPA2-PSK</b> or <b>WPA2</b> in the <b>Security Mode</b> field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for <b>WPA/WPA2</b> and <b>WPA-PSK/WPA2-PSK</b> are the same. The only difference between the two is that <b>WPA-PSK/WPA2-PSK</b> uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).  <b>Note:</b> If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).



**Table 26** Wireless: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK/WPA2-PSK</b> key management) or RADIUS server (if using <b>WPA/WPA2</b> key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in <b>WPA-PSK/WPA2-PSK</b> mode. The default is <b>1800</b> seconds (30 minutes).
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 5.4.4 WPA/WPA2

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

**Figure 46** Wireless: WPA/WPA2

The screenshot displays the 'General' tab of the Wireless LAN configuration interface. It is divided into two main sections: 'Wireless Setup' and 'Security'.

**Wireless Setup:**

- Enable Wireless LAN
- Name(SSID): ZyXEL
- Hide SSID
- Channel Selection: Channel-01 2412MHz
- Operating Channel: Channel-006

**Security:**

- Security Mode: WPA2
- WPA Compatible
- ReAuthentication Timer: 1800 (In Seconds)
- Idle Timeout: 3600 (In Seconds)
- Group Key Update Timer: 1800 (In Seconds)
- Authentication Server:
  - IP Address: 0.0.0.0
  - Port Number: 1812
  - Shared Secret: [Empty]
- Accounting Server:
  - Active
  - IP Address: 0.0.0.0
  - Port Number: 1813
  - Shared Secret: [Empty]

At the bottom of the page, there are two buttons: **Apply** and **Reset**.

The following table describes the labels in this screen.

**Table 27** Wireless: WPA/WPA2

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select <b>WPA2-PSK</b> or <b>WPA2</b> in the <b>Security Mode</b> field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).  Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK/WPA2-PSK</b> key management) or RADIUS server (if using <b>WPA/WPA2</b> key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in <b>WPA-PSK/WPA2-PSK</b> mode. The ZyXEL Device default is <b>1800</b> seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server	
Active	Select <b>Yes</b> from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 5.5 MAC Filter

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

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

**Figure 47** MAC Address Filter

MAC Address Filter

Active

Filter Action  Allow  Deny

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

Apply Reset

The following table describes the labels in this menu.

**Table 28** MAC Address Filter

LABEL	DESCRIPTION
Active	Select <b>Yes</b> from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the <b>MAC Address</b> table. Select <b>Deny</b> to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device Select <b>Allow</b> to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device.

**Table 28** MAC Address Filter

LABEL	DESCRIPTION
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 5.6 Wireless LAN Advanced Screen

Click **Network > Wireless LAN > Advanced**. The screen appears as shown.

**Figure 48** Wireless LAN Advanced

The following table describes the labels in this screen.

**Table 29** Wireless LAN Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. If the RTS/CTS value is greater than the <b>Fragmentation Threshold</b> value, then the RTS/CTS handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. Enter a value between 0 and 2432.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of APs within an area, decrease the output power of the ZyXEL Device to reduce interference with other APs.

**Table 29** Wireless LAN Advanced

LABEL	DESCRIPTION
802.11 Mode	Select <b>802.11b</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select <b>802.11g</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select <b>802.11b/g</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Super G Mode	Use this field to enable or disable the Super G function. Super G mode is available only if you select <b>802.11g</b> or <b>802.11b/g</b> in the <b>802.11 Mode</b> field. Super G provides higher data transmission rates than 802.11g. Select <b>Disabled</b> if your wireless clients do not support Super G. Select <b>Super G with Dynamic Turbo</b> if some or all of your wireless clients support Super G with Dynamic Turbo. Dynamic Turbo uses two channels bonded together to achieve higher transmission rates than 802.11g or Super G without Dynamic Turbo. Dynamic turbo is on only when all wireless devices on the network support it. The wireless channel is automatically fixed at 6 if you select this mode. Select <b>Super G without Turbo</b> if the wireless clients on your network support Super G but do not support dynamic turbo.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 5.7 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as e-mail, VoIP or FTP) a priority level.

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

Figure 49 Wireless LAN QoS

General MAC Filter Advanced **QoS**

QoS Setup

Enable WMM QoS

WMM QoS Policy: Application Priority

#	Name	Service	Dest Port	Priority	Modify
1	-	-	0	-	
2	-	-	0	-	
3	-	-	0	-	
4	-	-	0	-	
5	-	-	0	-	
6	-	-	0	-	
7	-	-	0	-	
8	-	-	0	-	
9	-	-	0	-	
10	-	-	0	-	
11	-	-	0	-	
12	-	-	0	-	
13	-	-	0	-	
14	-	-	0	-	
15	-	-	0	-	
16	-	-	0	-	

Apply

The following table describes the labels in this screen.

Table 30 Wireless LAN QoS

LABEL	DESCRIPTION
Enable WMM QoS	Select this to turn on WMM QoS (Wireless MultiMedia Quality of Service). The ZyXEL Device assigns priority to packets based on the 802.1q or DSCP information in their headers. If a packet has no WMM information in its header, it is assigned the default priority.
WMM QoS Policy	Select <b>Default</b> to have the ZyXEL Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Select <b>Application Priority</b> from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
	The table appears only if you select <b>Application Priority</b> in <b>WMM QoS Policy</b> .
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either <b>FTP</b> , <b>WWW</b> , <b>E-mail</b> or a <b>User Defined</b> service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.

**Table 30** Wireless LAN QoS (continued)

LABEL	DESCRIPTION
Priority	This field displays the priority of the application. <b>Highest</b> - Typically used for voice or video that should be high-quality. <b>High</b> - Typically used for voice or video that can be medium-quality. <b>Mid</b> - Typically used for applications that do not fit into another priority. For example, Internet surfing. <b>Low</b> - Typically used for non-critical “background” applications, such as large file transfers and print jobs that should not affect other applications.
Modify	Click the <b>Edit</b> icon to open the <b>Application Priority Configuration</b> screen. Modify an existing application entry or create a application entry in the <b>Application Priority Configuration</b> screen. Click the <b>Remove</b> icon to delete an application entry.
Apply	Click <b>Apply</b> to save your changes to the ZyXEL Device.

### 5.7.1 Application Priority Configuration

Use this screen to edit a WMM QoS application entry. Click the edit icon under **Modify**. The following screen displays.

**Figure 50** Application Priority Configuration

See [Appendix I on page 257](#) for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

**Table 31** Application Priority Configuration

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

**Table 31** Application Priority Configuration (continued)

LABEL	DESCRIPTION
Service	<p>The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box.</p> <ul style="list-style-type: none"> <li>• <b>E-Mail</b> Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80</li> <li>• <b>FTP</b> File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21.</li> <li>• <b>WWW</b> The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.</li> <li>• <b>User-Defined</b> User-defined services are user specific services configured using known ports and applications.</li> </ul>
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previous screen.



This chapter describes how to configure WAN settings.

## 6.1 WAN Overview

See the chapter about the connection wizard for more information on the fields in the WAN screens.

## 6.2 WAN MAC Address

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

## 6.3 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.

## 6.4 Internet Connection

Use this screen to change your ZyXEL Device's Internet access settings. Click **Network > WAN**. The screen differs according to the encapsulation you choose.

### 6.4.1 Ethernet Encapsulation

This screen displays when you select **Ethernet** encapsulation.

**Figure 51** Ethernet Encapsulation

The screenshot shows the 'Internet Connection' configuration page for a ZyXEL device, specifically the 'Advanced' tab. The page is divided into several sections:

- ISP Parameters for Internet Access:**
  - Encapsulation: Ethernet (selected in a dropdown menu)
  - Service Type: Standard (selected in a dropdown menu)
- WAN IP Address Assignment:**
  - Get automatically from ISP (Default)
  - Use Fixed IP Address
    - IP Address: 0.0.0.0
    - IP Subnet Mask: 0.0.0.0
    - Gateway IP Address: 0.0.0.0
- DNS Servers:**
  - First DNS Server: From ISP (dropdown), 172.23.5.1
  - Second DNS Server: From ISP (dropdown), 172.23.5.2
  - Third DNS Server: From ISP (dropdown), 0.0.0.0
- WAN MAC Address:**
  - Factory default
  - Clone the computer's MAC address - IP Address: 192.168.1.33
  - Set WAN MAC Address: 00:13:49:02:95:88

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

The following table describes the labels in this screen.

**Table 32** Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from <b>Standard</b> , <b>RR-Telstra</b> (RoadRunner Telstra authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method), <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method) or <b>Telia Login</b> . The following fields do not appear with the <b>Standard</b> service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one. This field is not available for <b>Telia Login</b> .
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example login1.telia.com.
Relogin Every(min) (Telia Login only)	The Telia server logs the ZyXEL Device out if the ZyXEL Device does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyXEL Device to wait between logins.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
IP Subnet Mask	Enter the <b>IP Subnet Mask</b> in this field.
Gateway IP Address	Enter a <b>Gateway IP Address</b> (if your ISP gave you one) in this field.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select <b>Factory default</b> to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select <b>Clone the computer's MAC address - IP Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.

**Table 32** Ethernet Encapsulation

LABEL	DESCRIPTION
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 6.4.2 PPPoE Encapsulation

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

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

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

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

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

This screen displays when you select **PPPoE** encapsulation.

Figure 52 PPPoE Encapsulation

The following table describes the labels in this screen.

Table 33 PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The <b>PPP over Ethernet</b> choice is for a dial-up connection using PPPoE. The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.

**Table 33** PPPoE Encapsulation

LABEL	DESCRIPTION
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
Remote IP Address	Enter the remote IP address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the remote IP subnet mask in this field.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the ZyXEL Device's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select <b>Factory default</b> to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select <b>Clone the computer's MAC address - IP Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 6.4.3 PPTP Encapsulation

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

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

This screen displays when you select **PPTP** encapsulation.

**Figure 53** PPTP Encapsulation

Internet Connection		Advanced
<b>ISP Parameters for Internet Access</b>		
Encapsulation	PPTP	
User Name		
Password	*****	
Retype to Confirm	*****	
<input type="checkbox"/> Nailed-Up Connection		
Idle Timeout (sec)	100	(in seconds)
<b>PPTP Configuration</b>		
<input type="radio"/> Get automatically from ISP (Default) <input checked="" type="radio"/> Use Fixed IP Address		
My IP Address	0.0.0.0	
My IP Subnet Mask	0.0.0.0	
Server IP Address	0.0.0.0	
Connection ID/Name		
<b>WAN IP Address Assignment</b>		
<input checked="" type="radio"/> Get automatically from ISP (Default) <input type="radio"/> Use Fixed IP Address		
My WAN IP Address	0.0.0.0	
Remote IP Address	0.0.0.0	
Remote IP Subnet Mask	0.0.0.0	
<b>DNS Servers</b>		
First DNS Server	From ISP	172.23.5.2
Second DNS Server	From ISP	172.23.5.1
Third DNS Server	From ISP	0.0.0.0
<b>WAN MAC Address</b>		
<input checked="" type="radio"/> Factory default <input type="radio"/> Clone the computer's MAC address - IP Address 192.168.1.33 <input type="radio"/> Set WAN MAC Address 00:13:49:a9:b1:29		
<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

The following table describes the labels in this screen.

**Table 34** PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyXEL Device supports only one PPTP server connection at any given time.  To configure a PPTP, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyXEL Device automatically disconnects from the PPTP server.
PPTP Configuration	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
Remote IP Address	Enter the remote IP address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the remote IP subnet mask in this field.
DNS Servers	



**Table 34** PPTP Encapsulation

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the ZyXEL Device's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select <b>Factory default</b> to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select <b>Clone the computer's MAC address - IP Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 6.5 Advanced WAN Screen

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

**Figure 54** WAN > Advanced

The screenshot shows the 'Advanced' configuration page for WAN settings. At the top, there are two tabs: 'Internet Connection' and 'Advanced', with 'Advanced' being the active tab. Below the tabs, there are three main sections: 'Multicast Setup', 'Windows Networking (NetBIOS over TCP/IP)', and a bottom section with 'Apply' and 'Reset' buttons. In the 'Multicast Setup' section, there is a 'Multicast' dropdown menu currently set to 'None'. In the 'Windows Networking' section, there are two checkboxes: 'Allow between LAN and WAN' and 'Allow Trigger Dial', both of which are currently unchecked.

The following table describes the labels in this screen.

**Table 35** WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Select <b>IGMP V-1</b> , <b>IGMP V-2</b> or <b>None</b> . IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. 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.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

This chapter describes how to configure LAN settings.

## 7.1 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, manage IP addresses, and partition your physical network into logical networks.

### 7.1.1 IP Pool Setup

The ZyXEL Device is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyXEL Device itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

### 7.1.2 System DNS Servers

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter.

## 7.2 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.

### 7.2.1 Factory LAN Defaults

The LAN parameters of the ZyXEL Device are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

## 7.2.2 IP Address and Subnet Mask

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter for this information.

## 7.2.3 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.

## 7.2.4 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.