

NBG318S

Powerline Ethernet Series

User's Guide

Version 3.6

4/2007

Edition 1



About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NBG318S 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 NBG318S.

- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Web Site
Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

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

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

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

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



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












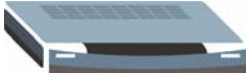
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NBG-318S may be referred to as the “NBG318S”, 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 NBG318S icon is not an exact representation of your device.

NBG318S 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 
Modem 		

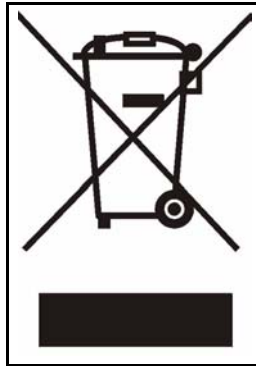
Safety Warnings



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

Introduction	29
Getting to Know Your NBG318S	31
Wireless Tutorial	35
Introducing the Web Configurator	43
Connection Wizard	55
Network	71
Wireless LAN	73
WAN	93
LAN	103
HomePlug AV	109
DHCP	115
Network Address Translation (NAT)	119
Dynamic DNS	129
Security	133
Firewall	135
Content Filtering	141
Management	147
Static Route Screens	149
Bandwidth Management	153
Remote Management	165
Universal Plug-and-Play (UPnP)	171
Maintenance and Troubleshooting	183
System	185
Logs	189
Tools	203
Configuration Mode	209
Sys Op Mode	211
Troubleshooting	213
Appendices and Index	221

Table of Contents

About This User's Guide	3
Document Conventions.....	4
Safety Warnings.....	6
Contents Overview	9
Table of Contents.....	11
List of Figures	19
List of Tables.....	25
Part I: Introduction.....	29
Chapter 1	
Getting to Know Your NBG318S.....	31
1.1 Overview	31
1.1.1 Secure Broadband Internet Access	31
1.1.2 Wireless LAN Application	32
1.1.3 HomePlug AV	32
1.2 Ways to Manage the NBG318S	33
1.3 Good Habits for Managing the NBG318S	33
1.4 LEDs	33
Chapter 2	
Wireless Tutorial.....	35
2.1 Example Parameters	35
2.2 Configuring the AP	35
2.3 Configuring the Wireless Client	37
2.3.1 Connecting to a Wireless LAN	37
2.3.2 Creating and Using a Profile	39
Chapter 3	
Introducing the Web Configurator	43
3.1 Web Configurator Overview	43
3.2 Accessing the Web Configurator	43
3.3 Resetting the NBG318S	45

3.3.1 Procedure to Use the Reset Button	45
3.4 Navigating the Web Configurator	45
3.4.1 The Status Screen	45
3.4.2 Navigation Panel	48
3.4.3 Summary: Any IP Table	50
3.4.4 Summary: Bandwidth Management Monitor	51
3.4.5 Summary: DHCP Table	51
3.4.6 Summary: Packet Statistics	52
3.4.7 Summary: Wireless Station Status	53
3.4.8 Summary: My HomePlug Network Status	53
Chapter 4	
Connection Wizard	55
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
Part II: Network.....	71
Chapter 5	
Wireless LAN.....	73
5.1 Wireless Network Overview	73
5.2 Wireless Security Overview	75
5.2.1 SSID	75
5.2.2 MAC Address Filter	75

5.2.3 User Authentication	76
5.2.4 Encryption	76
5.3 Roaming	77
5.3.1 Requirements for Roaming	78
5.4 Quality of Service	78
5.4.1 WMM QoS	79
5.5 General Wireless LAN Screen	79
5.5.1 No Security	80
5.5.2 WEP Encryption	81
5.5.3 WPA-PSK/WPA2-PSK	83
5.5.4 WPA/WPA2	84
5.6 MAC Filter	86
5.7 Wireless LAN Advanced Screen	87
5.8 Quality of Service (QoS) Screen	88
5.8.1 Application Priority Configuration	90
Chapter 6	
WAN	93
6.1 WAN Overview	93
6.2 WAN MAC Address	93
6.3 Multicast	93
6.4 Internet Connection	94
6.4.1 Ethernet Encapsulation	94
6.4.2 PPPoE Encapsulation	96
6.4.3 PPTP Encapsulation	98
6.5 Advanced WAN Screen	101
Chapter 7	
LAN.....	103
7.1 LAN Overview	103
7.1.1 IP Pool Setup	103
7.1.2 System DNS Servers	103
7.2 LAN TCP/IP	103
7.2.1 Factory LAN Defaults	103
7.2.2 IP Address and Subnet Mask	104
7.2.3 Multicast	104
7.2.4 Any IP	104
7.3 LAN IP Screen	106
7.4 LAN IP Alias	106
7.5 Advanced LAN Screen	107
Chapter 8	
HomePlug AV	109

8.1 Overview	109
8.2 Privacy and Powerline Adapters	110
8.2.1 Setting Up a Private Powerline Network	110
8.2.2 Setting Up Multiple Powerline Networks.	111
8.3 Configuring Your HomePlug AV Devices	112
Chapter 9	
DHCP	115
9.1 DHCP	115
9.2 DHCP Server General Screen	115
9.3 DHCP Server Advanced Screen	116
9.4 Client List Screen	117
Chapter 10	
Network Address Translation (NAT)	119
10.1 NAT Overview	119
10.2 Using NAT	119
10.2.1 Port Forwarding: Services and Port Numbers	119
10.2.2 Configuring Servers Behind Port Forwarding Example	120
10.3 General NAT Screen	120
10.4 NAT Application Screen	121
10.4.1 Game List Example	123
10.5 Trigger Port Forwarding	124
10.5.1 Trigger Port Forwarding Example	124
10.5.2 Two Points To Remember About Trigger Ports	125
10.6 NAT Advanced Screen	125
Chapter 11	
Dynamic DNS	129
11.1 Dynamic DNS Introduction	129
11.1.1 DynDNS Wildcard	129
11.2 Dynamic DNS Screen	129
Part III: Security	133
Chapter 12	
Firewall.....	135
12.1 Introduction to ZyXEL's Firewall	135
12.1.1 What is a Firewall?	135
12.1.2 Stateful Inspection Firewall	135
12.1.3 About the NBG318S Firewall	135

12.1.4 Guidelines For Enhancing Security With Your Firewall	136
12.2 Triangle Routes	136
12.2.1 Triangle Routes and IP Alias	136
12.3 General Firewall Screen	137
12.4 Services Screen	138
Chapter 13	
Content Filtering	141
13.1 Introduction to Content Filtering	141
13.2 Restrict Web Features	141
13.3 Days and Times	141
13.4 Filter Screen	141
13.5 Schedule	143
13.6 Customizing Keyword Blocking URL Checking	144
13.6.1 Domain Name or IP Address URL Checking	144
13.6.2 Full Path URL Checking	144
13.6.3 File Name URL Checking	144
Part IV: Management	147
Chapter 14	
Static Route Screens	149
14.1 Static Route Overview	149
14.2 IP Static Route Screen	149
14.2.1 Static Route Setup Screen	150
Chapter 15	
Bandwidth Management.....	153
15.1 Bandwidth Management Overview	153
15.2 Application-based Bandwidth Management	153
15.3 Subnet-based Bandwidth Management	153
15.4 Application and Subnet-based Bandwidth Management	154
15.5 Bandwidth Management Priorities	154
15.6 Predefined Bandwidth Management Services	155
15.6.1 Services and Port Numbers	156
15.7 Default Bandwidth Management Classes and Priorities	158
15.8 Bandwidth Management General Configuration	158
15.9 Bandwidth Management Advanced Configuration	159
15.9.1 Rule Configuration with the Pre-defined Service	160
15.9.2 Rule Configuration with the User-defined Service	161
15.10 Bandwidth Management Monitor	162

Chapter 16	
Remote Management.....	165
16.1 Remote Management Overview	165
16.1.1 Remote Management Limitations	165
16.1.2 Remote Management and NAT	166
16.1.3 System Timeout	166
16.2 WWW Screen	166
16.3 Telnet	166
16.4 Telnet Screen	167
16.5 FTP Screen	168
16.6 DNS Screen	168
Chapter 17	
Universal Plug-and-Play (UPnP).....	171
17.1 Introducing Universal Plug and Play	171
17.1.1 How do I know if I'm using UPnP?	171
17.1.2 NAT Traversal	171
17.1.3 Cautions with UPnP	171
17.2 UPnP and ZyXEL	172
17.3 UPnP Screen	172
17.4 Installing UPnP in Windows Example	173
Part V: Maintenance and Troubleshooting.....	183
Chapter 18	
System.....	185
18.1 System Overview	185
18.2 System General Screen	185
18.3 Time Setting Screen	186
Chapter 19	
Logs.....	189
19.1 View Log	189
19.2 Log Settings	190
19.3 Log Descriptions	193
Chapter 20	
Tools.....	203
20.1 Firmware Upload Screen	203
20.2 Configuration Screen	204
20.2.1 Backup Configuration	205

20.2.2 Restore Configuration	205
20.2.3 Back to Factory Defaults	206
20.3 Restart Screen	206
Chapter 21	
Configuration Mode	209
Chapter 22	
Sys Op Mode	211
22.1 Selecting System Operation Mode	211
Chapter 23	
Troubleshooting.....	213
23.1 Power, Hardware Connections, and LEDs	213
23.2 NBG318S Access and Login	214
23.3 Internet Access	215
23.4 Resetting the NBG318S to Its Factory Defaults	217
23.5 Wireless Router/AP Troubleshooting	217
23.6 HomePlug AV Troubleshooting	218
23.7 Advanced Features	219
Part VI: Appendices and Index	221
Appendix A Product Specifications and Wall-Mounting Instructions	223
Appendix B Pop-up Windows, JavaScripts and Java Permissions	229
Appendix C IP Addresses and Subnetting	235
Appendix D Setting up Your Computer's IP Address	243
23.7.1 Verifying Settings	258
Appendix E Wireless LANs	259
23.7.2 WPA(2)-PSK Application Example	268
23.7.3 WPA(2) with RADIUS Application Example	268
Appendix F Services	271
Appendix G Legal Information.....	275
Appendix H Customer Support.....	279
Index.....	283

List of Figures

Figure 1 Secure Internet Access	31
Figure 2 WLAN Application Example	32
Figure 3 HomePlug AV Internet Connection Example	32
Figure 4 Front Panel	33
Figure 5 Network > Wireless LAN > General	36
Figure 6 Network > Wireless LAN > General	36
Figure 7 AP: Status: WLAN Station Status	37
Figure 8 ZyXEL Utility: Security Settings	38
Figure 9 ZyXEL Utility: Confirm Save	39
Figure 10 ZyXEL Utility: Link Info	39
Figure 11 ZyXEL Utility: Profile	40
Figure 12 ZyXEL Utility: Add New Profile	40
Figure 13 ZyXEL Utility: Profile Security	40
Figure 14 ZyXEL Utility: Profile Encryption	41
Figure 15 Profile: Wireless Protocol Settings.	41
Figure 16 Profile: Confirm Save	41
Figure 17 Profile: Activate	42
Figure 18 Change Password Screen	44
Figure 19 Web Configurator Status Screen	46
Figure 20 Any IP Table	50
Figure 21 Summary: BW MGMT Monitor	51
Figure 22 Summary: DHCP Table	51
Figure 23 Summary: Packet Statistics	52
Figure 24 Summary: Wireless Association List	53
Figure 25 Summary: My Homeplug Network.	53
Figure 26 Select Wizard or Advanced Mode	55
Figure 27 Select a Language	56
Figure 28 Welcome to the Connection Wizard	56
Figure 29 Wizard Step 1: System Information	57
Figure 30 Wizard Step 2: Wireless LAN	58
Figure 31 Wizard Step 2: Basic (WEP) Security	59
Figure 32 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security	60
Figure 33 Wizard Step 3: ISP Parameters.	61
Figure 34 Wizard Step 3: Ethernet Connection	61
Figure 35 Wizard Step 3: PPPoE Connection	62
Figure 36 Wizard Step 3: PPTP Connection	63
Figure 37 Wizard Step 3: Your IP Address	64
Figure 38 Wizard Step 3: WAN IP and DNS Server Addresses	66

Figure 39 Wizard Step 3: WAN MAC Address	67
Figure 40 Wizard Step 4: Bandwidth Management	68
Figure 41 Connection Wizard Save	69
Figure 42 Connection Wizard Complete	69
Figure 43 Example of a Wireless Network	73
Figure 44 Roaming Example	78
Figure 45 Network > Wireless LAN > General	80
Figure 46 Network > Wireless LAN > General: No Security	81
Figure 47 Network > Wireless LAN > General: Static WEP	82
Figure 48 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK	83
Figure 49 Network > Wireless LAN > General: WPA/WPA2	84
Figure 50 Network > Wireless LAN > MAC Filter	86
Figure 51 Network > Wireless LAN > Advanced	87
Figure 52 Network > Wireless LAN > QoS	89
Figure 53 Network > Wireless LAN > QoS: Application Priority Configuration	90
Figure 54 Network > WAN > Internet Connection: Ethernet Encapsulation	94
Figure 55 Network > WAN > Internet Connection: PPPoE Encapsulation	97
Figure 56 Network > WAN > Internet Connection: PPTP Encapsulation	99
Figure 57 Network > WAN > Advanced	101
Figure 58 Any IP Example	105
Figure 59 Network > LAN > IP	106
Figure 60 Network > LAN > IP Alias	107
Figure 61 Network > LAN > Advanced	107
Figure 62 Expand Your Network	109
Figure 63 Powerline Network Scenario	111
Figure 64 Two Private Powerline Networks on One Circuit	112
Figure 65 Network > HomePlug > Network Settings	112
Figure 66 Network > HomePlug > Edit	114
Figure 67 Network > DHCP Server > General	115
Figure 68 Network > DHCP Server > Advanced	116
Figure 69 Network > DHCP Server > Client List	117
Figure 70 Multiple Servers Behind NAT Example	120
Figure 71 Network > NAT > General	120
Figure 72 Network > NAT > Application	122
Figure 73 Game List Example	124
Figure 74 Trigger Port Forwarding Process: Example	125
Figure 75 Network > NAT > Advanced	126
Figure 76 Dynamic DNS	130
Figure 77 Using IP Alias to Solve the Triangle Route Problem	137
Figure 78 Security > Firewall > General I	137
Figure 79 Security > Firewall > Services	139
Figure 80 Security > Content Filter > Filter	142
Figure 81 Security > Content Filter > Schedule	143

Figure 82 Example of Static Routing Topology	149
Figure 83 Management > Static Route > IP Static Route	150
Figure 84 Management > Static Route > IP Static Route: Static Route Setup	151
Figure 85 Subnet-based Bandwidth Management Example	154
Figure 86 Management > Bandwidth MGMT > General	158
Figure 87 Management > Bandwidth MGMT > Advanced	159
Figure 88 Management > Bandwidth MGMT > Advanced: Rule Configuration	161
Figure 89 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration ..	162
Figure 90 Management > Bandwidth MGMT > Monitor	163
Figure 91 Management > Remote MGMT > WWW	166
Figure 92 Telnet Configuration on a TCP/IP Network	167
Figure 93 Management > Remote MGMT > Telnet	167
Figure 94 Management > Remote MGMT > FTP	168
Figure 95 Management > Remote MGMT > DNS	169
Figure 96 Management > UPnP > General	172
Figure 97 Add/Remove Programs: Windows Setup: Communication	173
Figure 98 Add/Remove Programs: Windows Setup: Communication: Components	174
Figure 99 Network Connections	174
Figure 100 Windows Optional Networking Components Wizard	175
Figure 101 Networking Services	175
Figure 102 Network Connections	176
Figure 103 Internet Connection Properties	177
Figure 104 Internet Connection Properties: Advanced Settings	178
Figure 105 Internet Connection Properties: Advanced Settings: Add	178
Figure 106 System Tray Icon	179
Figure 107 Internet Connection Status	179
Figure 108 Network Connections	180
Figure 109 Network Connections: My Network Places	181
Figure 110 Network Connections: My Network Places: Properties: Example	181
Figure 111 Maintenance > System > General	185
Figure 112 Maintenance > System > Time Setting	187
Figure 113 Maintenance > Logs > View Log	189
Figure 114 Maintenance > Logs > Log Settings	191
Figure 115 Maintenance > Tools > Firmware	203
Figure 116 Upload Warning	204
Figure 117 Network Temporarily Disconnected	204
Figure 118 Upload Error Message	204
Figure 119 Maintenance > Tools > Configuration	205
Figure 120 Configuration Restore Successful	206
Figure 121 Temporarily Disconnected	206
Figure 122 Configuration Restore Error	206
Figure 123 Maintenance > Tools > Restart	207
Figure 124 Maintenance > Config Mode > General	209

Figure 125 Maintenance > Sys OP Mode > General	211
Figure 126 System Operation Mode: Ethernet WAN	211
Figure 127 System Operation Mode: HomePlug WAN	212
Figure 128 Wall-mounting Example	227
Figure 129 Masonry Plug and M4 Tap Screw	227
Figure 130 Pop-up Blocker	229
Figure 131 Internet Options: Privacy	230
Figure 132 Internet Options: Privacy	231
Figure 133 Pop-up Blocker Settings	231
Figure 134 Internet Options: Security	232
Figure 135 Security Settings - Java Scripting	233
Figure 136 Security Settings - Java	233
Figure 137 Java (Sun)	234
Figure 138 Network Number and Host ID	236
Figure 139 Subnetting Example: Before Subnetting	238
Figure 140 Subnetting Example: After Subnetting	239
Figure 141 WIndows 95/98/Me: Network: Configuration	244
Figure 142 Windows 95/98/Me: TCP/IP Properties: IP Address	245
Figure 143 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	246
Figure 144 Windows XP: Start Menu	247
Figure 145 Windows XP: Control Panel	247
Figure 146 Windows XP: Control Panel: Network Connections: Properties	248
Figure 147 Windows XP: Local Area Connection Properties	248
Figure 148 Windows XP: Internet Protocol (TCP/IP) Properties	249
Figure 149 Windows XP: Advanced TCP/IP Properties	250
Figure 150 Windows XP: Internet Protocol (TCP/IP) Properties	251
Figure 151 Macintosh OS 8/9: Apple Menu	252
Figure 152 Macintosh OS 8/9: TCP/IP	252
Figure 153 Macintosh OS X: Apple Menu	253
Figure 154 Macintosh OS X: Network	254
Figure 155 Red Hat 9.0: KDE: Network Configuration: Devices	255
Figure 156 Red Hat 9.0: KDE: Ethernet Device: General	256
Figure 157 Red Hat 9.0: KDE: Network Configuration: DNS	256
Figure 158 Red Hat 9.0: KDE: Network Configuration: Activate	257
Figure 159 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	257
Figure 160 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	257
Figure 161 Red Hat 9.0: DNS Settings in resolv.conf	258
Figure 162 Red Hat 9.0: Restart Ethernet Card	258
Figure 163 Red Hat 9.0: Checking TCP/IP Properties	258
Figure 164 Peer-to-Peer Communication in an Ad-hoc Network	259
Figure 165 Basic Service Set	260
Figure 166 Infrastructure WLAN	261
Figure 167 RTS/CTS	262

Figure 168 WPA(2)-PSK Authentication 268

List of Tables

Table 1 Front Panel LEDs	33
Table 2 Status Screen Icon Key	46
Table 3 Web Configurator Status Screen	47
Table 4 Screens Summary	48
Table 5 Summary: DHCP Table	51
Table 6 Summary: Packet Statistics	52
Table 7 Summary: Wireless Association List	53
Table 8 Summary: My Homeplug Network	54
Table 9 Wizard Step 1: System Information	57
Table 10 Wizard Step 2: Wireless LAN	58
Table 11 Wizard Step 2: Basic (WEP) Security	59
Table 12 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security	60
Table 13 Wizard Step 3: ISP Parameters	61
Table 14 Wizard Step 3: PPPoE Connection	62
Table 15 Wizard Step 3: PPTP Connection	63
Table 16 Wizard Step 3: Your IP Address	64
Table 17 Private IP Address Ranges	64
Table 18 Wizard Step 3: WAN IP and DNS Server Addresses	66
Table 19 Example of Network Properties for LAN Servers with Fixed IP Addresses	67
Table 20 Wizard Step 3: WAN MAC Address	67
Table 21 Wizard Step 4: Bandwidth Management	68
Table 22 Types of Encryption for Each Type of Authentication	76
Table 23 WMM QoS Priorities	79
Table 24 Network > Wireless LAN > General	80
Table 25 Wireless No Security	81
Table 26 Network > Wireless LAN > General: Static WEP	82
Table 27 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK	83
Table 28 Network > Wireless LAN > General: WPA/WPA2	85
Table 29 Network > Wireless LAN > MAC Filter	86
Table 30 Network > Wireless LAN > Advanced	87
Table 31 Network > Wireless LAN > QoS	89
Table 32 Network > Wireless LAN > QoS: Application Priority Configuration	90
Table 33 Network > WAN > Internet Connection: Ethernet Encapsulation	95
Table 34 Network > WAN > Internet Connection: PPPoE Encapsulation	97
Table 35 Network > WAN > Internet Connection: PPTP Encapsulation	100
Table 36 WAN > Advanced	102
Table 37 Network > LAN > IP	106
Table 38 Network > LAN > IP Alias	107

Table 39 Network > LAN > Advanced	108
Table 40 Network > HomePlug > Network Settings	113
Table 41 Network > HomePlug > Edit	114
Table 42 Network > DHCP Server > General	115
Table 43 Network > DHCP Server > Advanced	116
Table 44 Network > DHCP Server > Client List	118
Table 45 Network > NAT > General	121
Table 46 NAT Application	122
Table 47 Network > NAT > Advanced	126
Table 48 Dynamic DNS	130
Table 49 Security > Firewall > General	137
Table 50 Security > Firewall > Services	139
Table 51 Security > Content Filter > Filter	142
Table 52 Security > Content Filter > Schedule	143
Table 53 Management > Static Route > IP Static Route	150
Table 54 Management > Static Route > IP Static Route: Static Route Setup	151
Table 55 Application and Subnet-based Bandwidth Management Example	154
Table 56 Bandwidth Management Priorities	154
Table 57 Media Bandwidth Management Setup: Services	155
Table 58 Commonly Used Services	156
Table 59 Bandwidth Management Priority with Default Classes	158
Table 60 Management > Bandwidth MGMT > General	159
Table 61 Management > Bandwidth MGMT > Advanced	160
Table 62 Management > Bandwidth MGMT > Advanced: Application Rule Configuration	161
Table 63 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration	162
Table 64 Management > Remote MGMT > WWW	166
Table 65 Management > Remote MGMT > Telnet	167
Table 66 Management > Remote MGMT > FTP	168
Table 67 Management > Remote MGMT > DNS	169
Table 68 Management > UPnP > General	172
Table 69 Maintenance > System > General	186
Table 70 Maintenance > System > Time Setting	187
Table 71 Maintenance > Logs > View Log	190
Table 72 Maintenance > Logs > Log Settings	191
Table 73 System Maintenance Logs	193
Table 74 System Error Logs	194
Table 75 Access Control Logs	194
Table 76 TCP Reset Logs	194
Table 77 Packet Filter Logs	195
Table 78 ICMP Logs	195
Table 79 CDR Logs	196
Table 80 PPP Logs	196
Table 81 UPnP Logs	196

Table 82 Content Filtering Logs	196
Table 83 Attack Logs	197
Table 84 PKI Logs	198
Table 85 802.1X Logs	199
Table 86 ACL Setting Notes	200
Table 87 ICMP Notes	200
Table 88 Syslog Logs	201
Table 89 RFC-2408 ISAKMP Payload Types	201
Table 90 Maintenance > Tools > Firmware	203
Table 91 Maintenance Restore Configuration	205
Table 92 Maintenance > Config Mode > General	209
Table 93 Advanced Configuration Options	210
Table 94 Maintenance > Sys OP Mode > General	212
Table 95 Hardware Features	223
Table 96 Firmware Features	224
Table 97 Standards Supported	225
Table 98 Subnet Mask - Identifying Network Number	236
Table 99 Subnet Masks	237
Table 100 Maximum Host Numbers	237
Table 101 Alternative Subnet Mask Notation	237
Table 102 Subnet 1	239
Table 103 Subnet 2	240
Table 104 Subnet 3	240
Table 105 Subnet 4	240
Table 106 Eight Subnets	240
Table 107 24-bit Network Number Subnet Planning	241
Table 108 16-bit Network Number Subnet Planning	241
Table 109 IEEE 802.11g	263
Table 110 Comparison of EAP Authentication Types	266
Table 111 Wireless Security Relational Matrix	269
Table 112 Examples of Services	271

PART I

Introduction

Getting to Know Your NBG318S (31)
Wireless Tutorial (35)
Introducing the Web Configurator (43)
Connection Wizard (55)

Getting to Know Your NBG318S

This chapter introduces the main features and applications of the NBG318S.

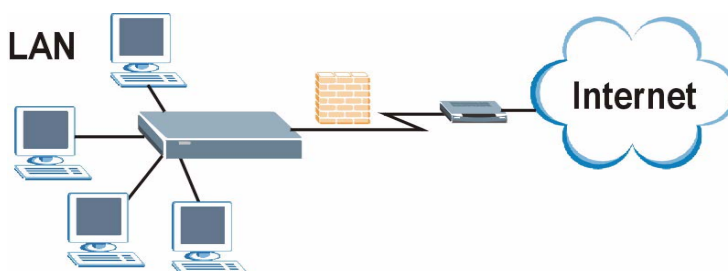
1.1 Overview

The NBG318S is the ideal secure HomePlug AV wireless firewall router for all data passing between the Internet and your local network.

1.1.1 Secure Broadband Internet Access

Connect a broadband modem to your NBG318S for shared Internet access protected by firewall and content filtering. 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 Voice over Internet (VoIP).

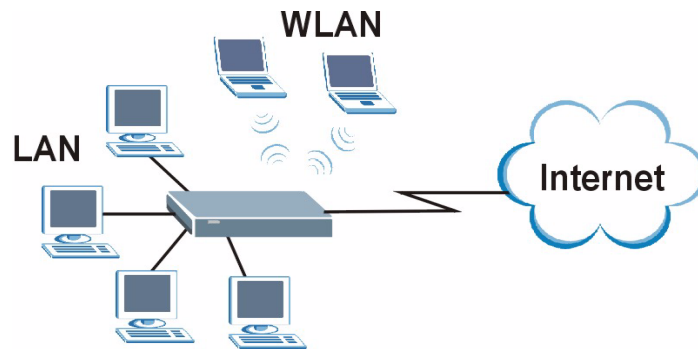
Figure 1 Secure Internet Access



1.1.2 Wireless LAN Application

The NBG318S Wireless LAN feature allows IEEE 802.11b or IEEE 802.11g compatible wireless clients to access the Internet or the local network as well as to communicate with each other. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network. The Super G function allows compatible clients to connect to the NBG318S at up to 108 Mbps.

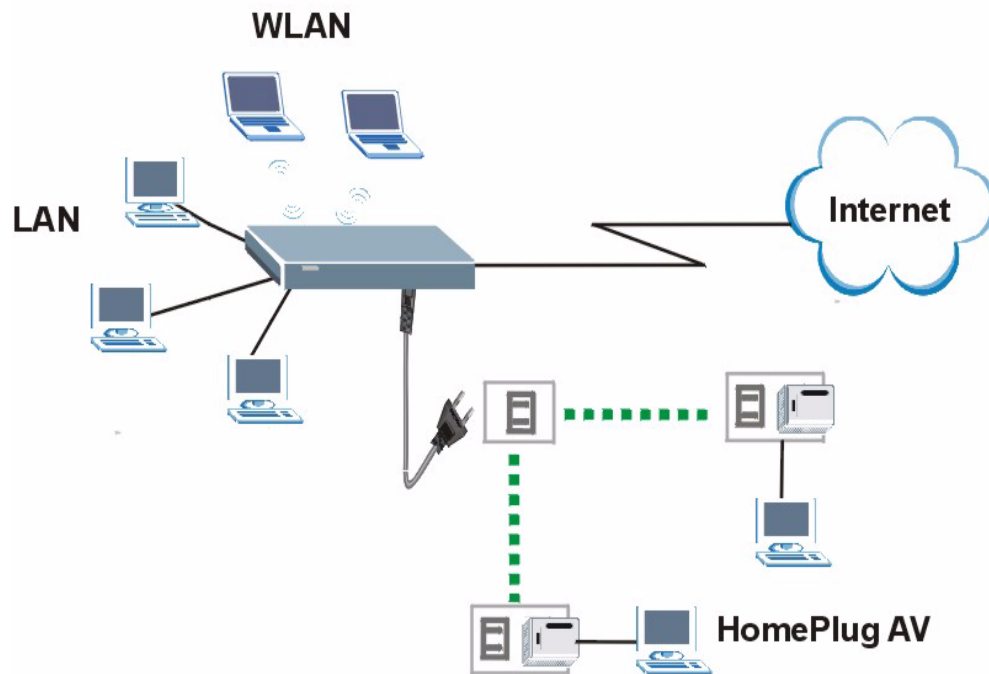
Figure 2 WLAN Application Example



1.1.3 HomePlug AV

Connect to other HomePlug AV compatible devices through your home electrical wiring. A HomePlug AV network is capable of up to 200Mbps data transfer without the need for network cables.

Figure 3 HomePlug AV Internet Connection Example



1.2 Ways to Manage the NBG318S

Use any of the following methods to manage the NBG318S.

- Web Configurator. This is recommended for everyday management of the NBG318S 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.

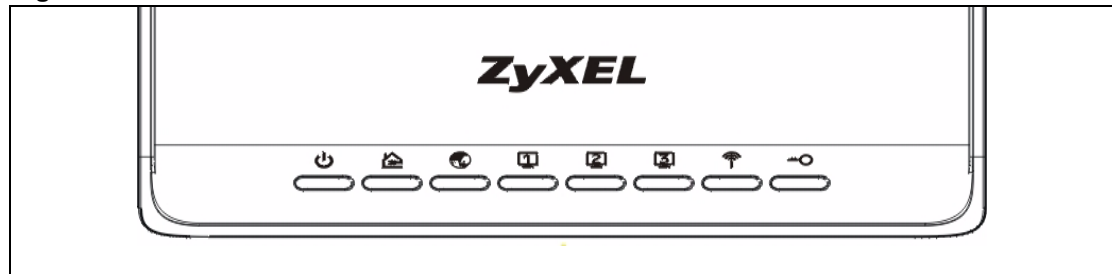
1.3 Good Habits for Managing the NBG318S

Do the following things regularly to make the NBG318S more secure and to manage the NBG318S 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 NBG318S to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG318S. You could simply restore your last configuration.

1.4 LEDs

Figure 4 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs









LED	ICON	COLOR	STATUS	DESCRIPTION
POWER		Green	On	The NBG318S is receiving power and functioning properly.
			Off	The NBG318S is not receiving power.
HomePlug		Green	On	The NBG318S has a successful HomePlug AV connection.
			Blinking	The NBG318S is sending/receiving data.
			Off	The HomePlug AV connection is not ready, or failed.

Table 1 Front Panel LEDs (continued)

LED	ICON	COLOR	STATUS	DESCRIPTION
WAN		Green	On	The NBG318S has a successful 10Mb WAN connection.
			Blinking	The NBG318S is sending/receiving data.
		Amber	On	The NBG318S has a successful 100Mb Ethernet connection.
			Blinking	The NBG318S is sending/receiving data.
		None	Off	The WAN connection is not ready, or has failed.
LAN 1-3	  	Green	On	The NBG318S has a successful 10Mb Ethernet connection.
			Blinking	The NBG318S is sending/receiving data.
		Amber	On	The NBG318S has a successful 100Mb Ethernet connection.
			Blinking	The NBG318S is sending/receiving data.
			Off	The LAN is not connected.
WLAN		Green	On	The NBG318S is ready, but is not sending/receiving data through the wireless LAN.
			Blinking	The NBG318S is sending/receiving data through the wireless LAN.
		None	Off	The wireless LAN is not ready or has failed.
WPS		WPS means WiFi Protected Setup. WPS automatically sets up security on your wireless network. This LED is reserved for future use.		

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

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	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 5 Network > 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 6 Network > Wireless LAN > General

Status

Device Information

System Name: NBG-318S
Firmware Version: V3.60(AMR.0)pre-b1 | 02/16/2007

WAN Information

- MAC Address: 00:19:cb:00:00:02
- IP Address: 0.0.0.0
- IP Subnet Mask: 0.0.0.0
- DHCP: None

LAN Information

- MAC Address: 00:19:cb:00:00:01
- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0

WLAN Information

- MAC Address: 00:19:cb:00:00:01
- Name(SSID): ZyXEL
- Channel: 6
- Operating Channel: 6
- Security Mode: No Security
- Super G Mode: Disabled

HomePlug Information

- Firmware Version: INT6000-MAC-1-4-1424-531-20060918-FINAL-B

System Status

System Up Time: 2:35:25
Current Date/Time: 2000-1-1/2:35:22

System Resource

- CPU Usage: 4.96%
- Memory Usage: 50%

System Setting

- Firewall: Enabled
- Bandwidth Management: Enabled
- UPnP: Enabled
- Configuration Mode: Advanced

Interface Status

Interface	Status	Rate
WAN	Up	Dial
LAN	Up	100M/Full
WLAN	Up	54M
HomePlug AV	Up	200M

Summary

Any IP Table ([Details...](#))
 BW MGMT Monitor ([Details...](#))
 DHCP Table ([Details...](#))
 WLAN Station Status ([Details...](#))
 My HomePlug Network ([Details...](#))

- 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 7 AP: Status: WLAN Station Status

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

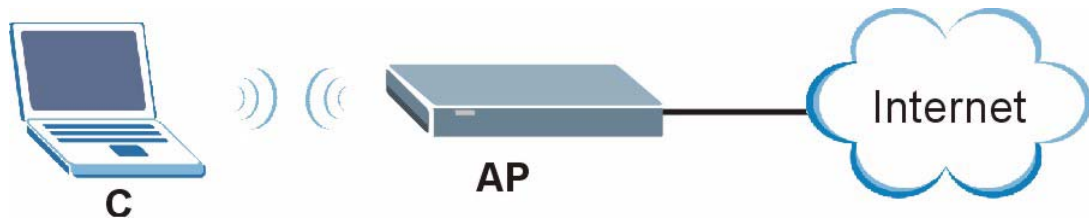
Refresh

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 labelled **C** and the access point is labelled **AP**.



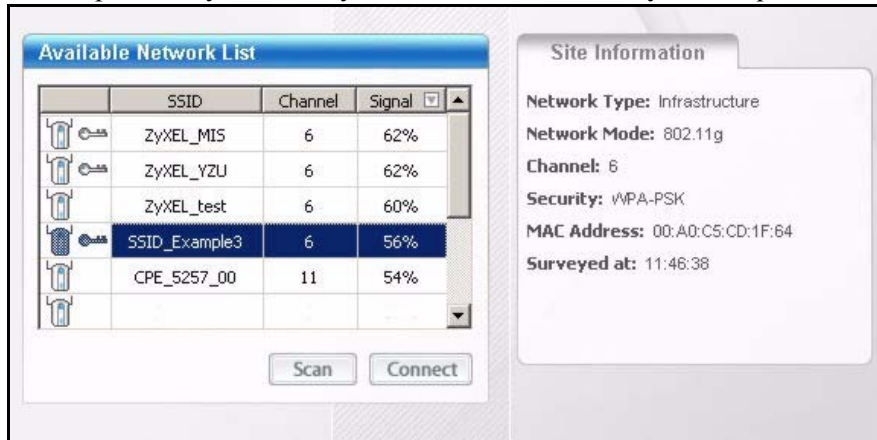
There are three ways to connect the client to an access point.

- 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”.

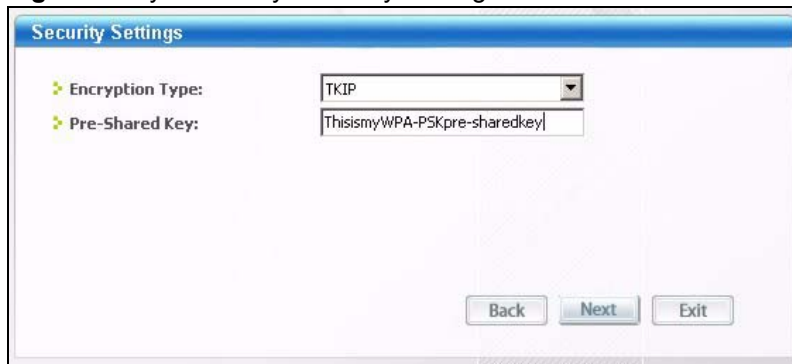
After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

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

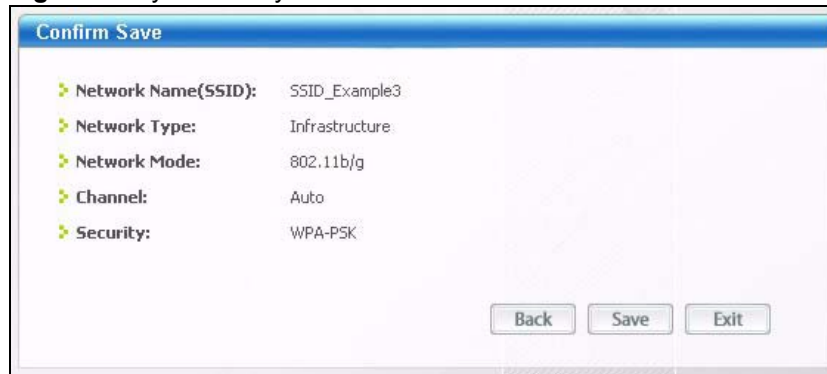


- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the 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.

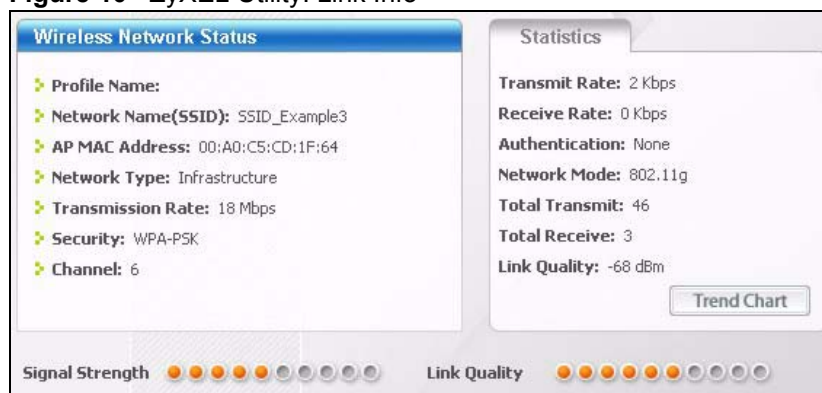
Figure 8 ZyXEL Utility: Security Settings



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

Figure 9 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 10 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.

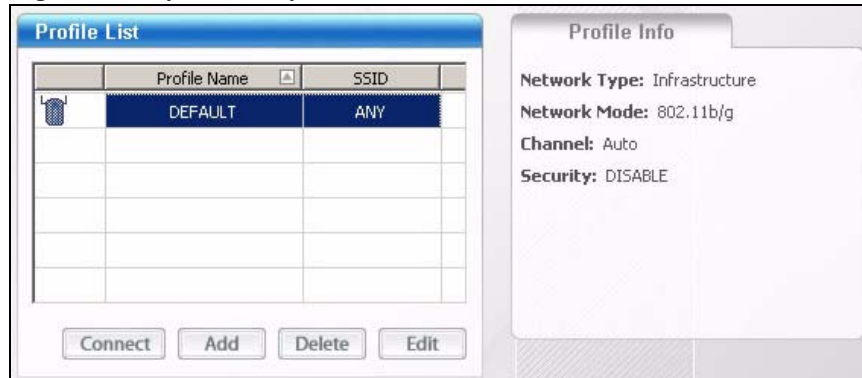
2.3.2 Creating and Using a Profile

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”.

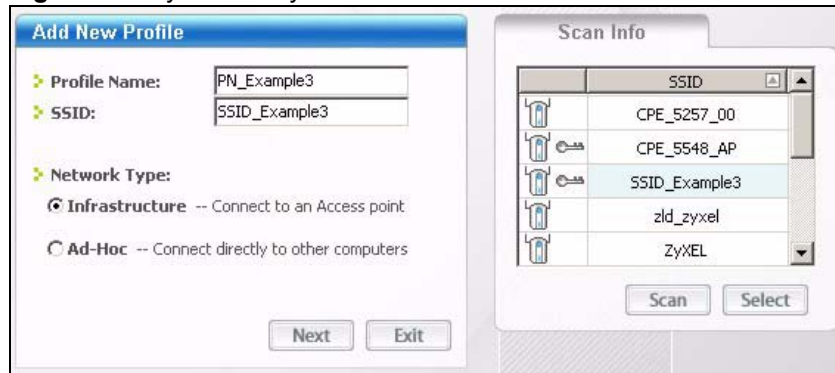
- 1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.

Figure 11 ZyXEL Utility: Profile



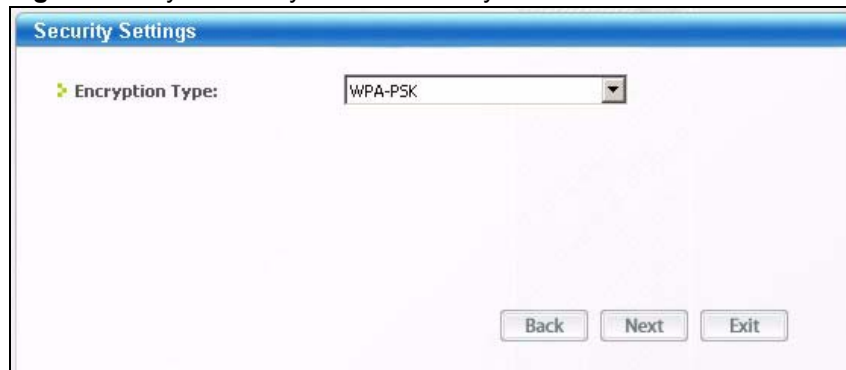
- 2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. Click on **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.

Figure 12 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 13 ZyXEL Utility: Profile Security



- 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 14 ZyXEL Utility: Profile Encryption

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

Figure 15 Profile: Wireless Protocol Settings.

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

Figure 16 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 17 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 NBG318S 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 NBG318S 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 NBG318S hardware is properly connected and prepare your computer or computer network to connect to the NBG318S (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "http://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 18 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.

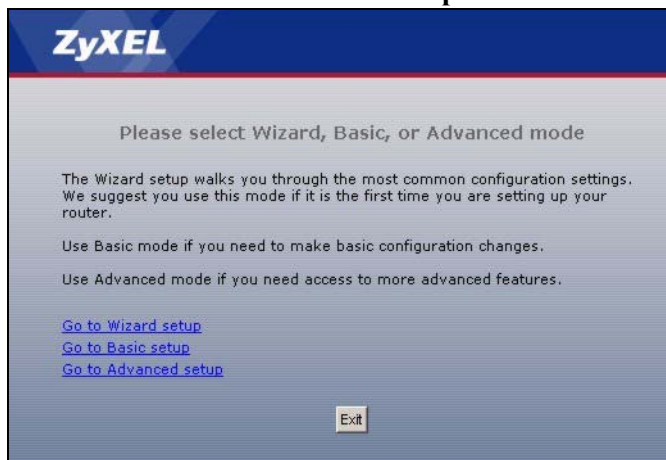
New Password:

Retype to Confirm:



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 NBG318S 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 NBG318S'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](#)

[Go to Basic setup](#)

[Go to Advanced setup](#)

3.3 Resetting the NBG318S

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the NBG318S 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 NBG318S 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 NBG318S.



Not all fields are available when you select **Basic** mode (see [Section 3.2 on page 43](#)). 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 19 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 None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	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 System Name you enter in the Maintenance > System > General 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 - Client or None .
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 - Server or None .
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 NBG318S in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG318S is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG318S is using.
- 802.11 Mode	This shows the wireless standard.
- Super G Mode	This shows whether SuperG is enabled or not.
HomePlug Information	
- MAC Address	This shows the MAC Address of your device.
System Status	
System Uptime	This is the total time the NBG318S has been on.
Current Date/Time	This field displays your NBG318S's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG318S's processing ability is currently used. When this percentage is close to 100%, the NBG318S 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 NBG318S 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.

Table 3 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
- UPnP	This shows whether UPnP is active or not.
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (Advanced) or not (Basic).
Interface Status	
Interface	This displays the NBG318S port types. The port types are: WAN , LAN , HomePlug AV and WLAN .
Status	For the LAN and WAN ports, this field displays Down (line is down) or Up (line is up or connected). For the WLAN, it displays Up when the WLAN is enabled or Down when the WLAN is disabled. For the HomePlug AV port it displays Up when the power cord is connected.
Rate	For the LAN ports, this displays the port speed and duplex setting or N/A when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and Idle (line ppp idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays N/A when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled. For the HomePlug AV port it displays the maximum transmission rate when the HomePlug AV is enabled.
Summary	
Any IP Table	Use this screen to view details of IP addresses assigned to devices not in the same subnet as the NBG318S.
BW MGMT Monitor	Use this screen to view the NBG318S'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 NBG318S.
My HomePlug Network	Use this screen to view information on the stations connected to your Home Plug network.

3.4.2 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure NBG318S features.

The following table describes the sub-menus.

Table 4 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG318S's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		

Table 4 Screens Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG318S to block access to devices or block the devices from accessing the NBG318S.
	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.
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.
HomePlug	Network Settings	Use this screen to configure HomePlug AV devices and set up a power line network.
DHCP Server	General	Use this screen to enable the NBG318S'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 NBG318S.
	Advanced	Use this screen to change your NBG318S'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 NBG318S 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 NBG318S's bandwidth usage and allotments.

Table 4 Screens Summary

LINK	TAB	FUNCTION
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 NBG318S.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG318S.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the NBG318S.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the NBG318S.
UPnP	General	Use this screen to enable UPnP on the NBG318S.
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 NBG318S'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 NBG318S's log settings.
Tools	Firmware	Use this screen to upload firmware to your NBG318S.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG318S.
	Restart	This screen allows you to reboot the NBG318S without turning the power off.
Config Mode	General	This screen allows you to display or hide the advanced screens or features.
Sys OP Mode	General	This screen allows you to select either an Ethernet or a HomePlug AV WAN connection to the Internet.

3.4.3 Summary: Any IP Table

This screen displays the IP address of each computer that is using the NBG318S via the any IP feature. Any IP allows computers to access the Internet through the NBG318S without changing their network settings when NAT is enabled. To access this screen, open the **Status** screen (see [Section 3.4.1 on page 45](#)), and click **(Details...)** next to **Any IP Table**.

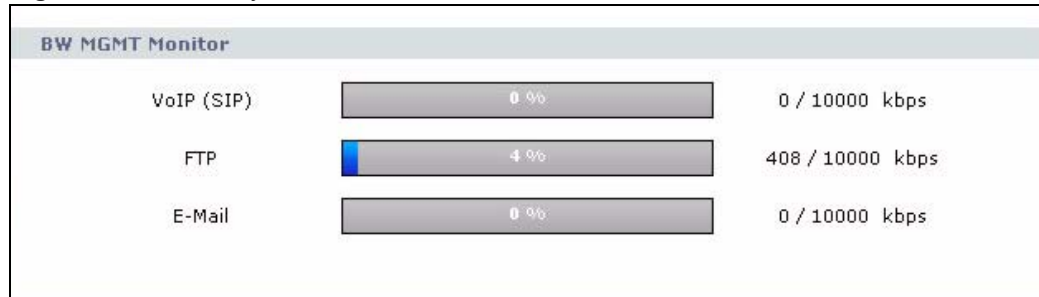
Figure 20 Any IP Table

Any IP TABLE		
#	IP Address	MAC Address
.....		
Refresh		

3.4.4 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 21 Summary: BW MGMT Monitor



3.4.5 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 NBG318S as a DHCP server or disable it. When configured as a server, the NBG318S 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 NBG318S's DHCP server.

Figure 22 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.

Table 5 Summary: DHCP Table (continued)

LABEL	DESCRIPTION
MAC Address	This field shows the MAC address of the computer with the name in the Host Name 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 Refresh to renew the screen.

3.4.6 Summary: Packet Statistics

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

Figure 23 Summary: 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) : 5 sec

The following table describes the labels in this screen.

Table 6 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG318S's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or Down when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays Down when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and Down 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 NBG318S has been on.

Table 6 Summary: Packet Statistics

LABEL	DESCRIPTION
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 Poll Interval(s) field.
Stop	Click Stop to stop refreshing statistics.

3.4.7 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 NBG318S in the **Association List** screen.

Figure 24 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 NBG318S.
Refresh	Click Refresh to reload the list.

3.4.8 Summary: My HomePlug Network Status

Click the **My HomePlug Network (Details...)** hyperlink in the **Status** screen. View the powerline stations that are currently associated to the NBG318S in the **My Homeplug Network** screen.

Figure 25 Summary: My Homeplug Network.

My HomePlug Network	
Site	MAC Address
Local	00:13:49:D1:CB:88
Remote	00:13:49:EA:F0:BE

Refresh

The following table describes the labels in this screen.

Table 8 Summary: My Homeplug Network

LABEL	DESCRIPTION
Site	Your NBG318S is the Local device. All other devices on your network will be Remote .
MAC Address	This field displays the MAC address of a HomePlug AV device detected by your NBG318S.
Refresh	Click Refresh to reload the list.

Connection Wizard

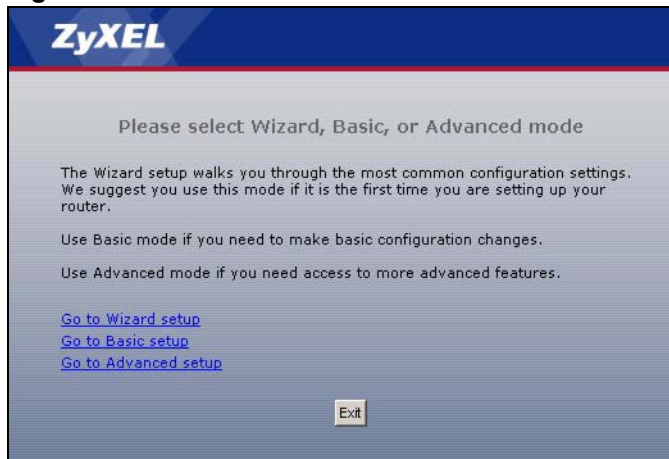
This chapter provides information on the wizard setup screens in the web configurator.

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 NBG318S 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 26 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 27 Select a Language



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

Figure 28 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 NBG318S **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 NBG318S via DHCP.

Click **Next** to configure the NBG318S for Internet access.

Figure 29 Wizard Step 1: System Information

The following table describes the labels in this screen.

Table 9 Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG318S 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 Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

4.3 Connection Wizard: STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

Figure 30 Wizard Step 2: Wireless LAN

The following table describes the labels in this screen.

Table 10 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 NBG318S, make sure all wireless stations use the same SSID in order to access the network.
Security	Select a Security level from the drop-down list box. Choose Auto to have the NBG318S generate a pre-shared key automatically. A screen pops up displaying the generated pre-shared key after you click Next . Write down the key for use later when connecting other wireless devices to your network. Click OK to continue. Choose None to have no wireless LAN security configured. If you do not enable any wireless security on your NBG318S, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to Section 4.4 on page 60 . Choose Basic (WEP) security if you want to configure WEP Encryption parameters. If you choose this option, go directly to Section 4.3.1 on page 59 . Choose Extend (WPA-PSK or WPA2-PSK) 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 Section 4.3.2 on page 60 .
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 Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.



The wireless stations and NBG318S 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 31 Wizard Step 2: Basic (WEP) Security

STEP 1 ▶ STEP 2 ▶ STEP 3 ▶ STEP 4

WIRELESS LAN

Passphrase

Use Passphrase to automatically generates a WEP key.

Passphrase

WEP Key

The higher the WEP Encryption, the higher the security but the slower the throughput. Select 64-bit WEP, 128-bit WEP or 256-bit WEP to enable data encryption and select one of the Key radio buttons to use as the WEP key. Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.

WEP Encryption

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 labels in this screen.

Table 11 Wizard Step 2: Basic (WEP) Security

LABEL	DESCRIPTION
Passphrase	Type a Passphrase (up to 32 printable characters) and click Generate . The NBG318S automatically generates a WEP key.
WEP Encryption	Select 64-bit WEP or 128-bit WEP 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 NBG318S and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP , 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 Back to display the previous screen.

Table 11 Wizard Step 2: Basic (WEP) Security

LABEL	DESCRIPTION
Next	Click Next to proceed to the next screen.
Exit	Click Exit 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 32 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

The following table describes the labels in this screen.

Table 12 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 Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

4.4 Connection Wizard: STEP 3: Internet Configuration

The NBG318S 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 33 Wizard Step 3: ISP Parameters.

The following table describes the labels in this screen,

Table 13 Wizard Step 3: ISP Parameters

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

4.4.1 Ethernet Connection

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

Figure 34 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 NBG318S (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG318S 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 35 Wizard Step 3: PPPoE Connection

The following table describes the labels in this screen.

Table 14 Wizard Step 3: PPPoE Connection

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Connection Type	Select the PPP over Ethernet 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 Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit 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 NBG318S supports one PPTP server connection at any given time.

Figure 36 Wizard Step 3: PPTP Connection

The following table describes the fields in this screen

Table 15 Wizard Step 3: PPTP Connection

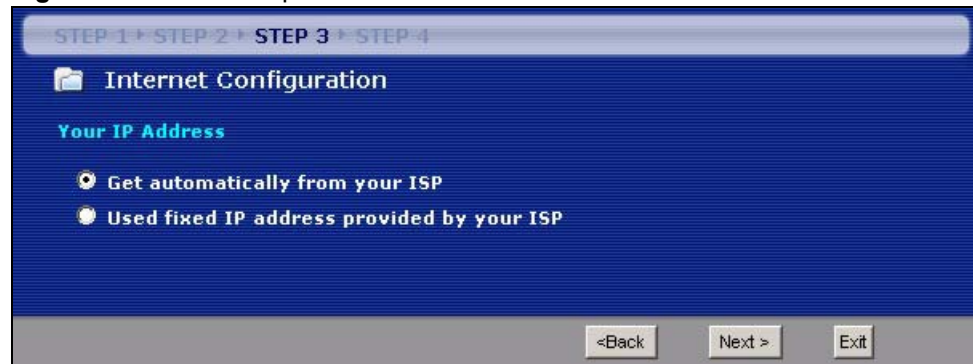
LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select PPTP from the drop-down list box. To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you 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 NBG318S 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 Back to return to the previous screen.

Table 15 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
Next	Click Next to continue.
Exit	Click Exit 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 NBG318S an automatically assigned IP address depending on your ISP.

Figure 37 Wizard Step 3: Your IP Address

The following table describes the labels in this screen

Table 16 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 4.4.9 .
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 Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit 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 17 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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



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

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 NBG318S, 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 NBG318S 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 NBG318S 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 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 NBG318S 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 38 Wizard Step 3: WAN IP and DNS Server Addresses

The screenshot shows a wizard window 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 18 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 NBG318S 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 Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

4.4.9 WAN MAC Address

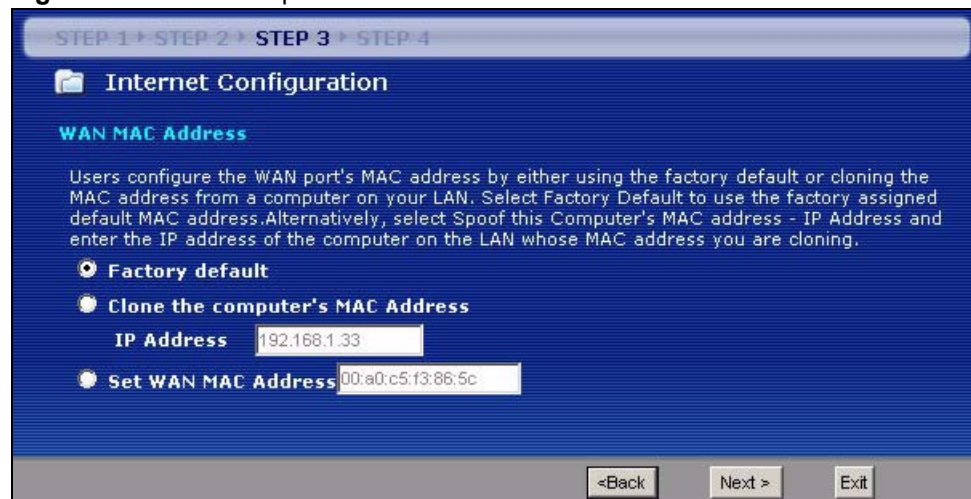
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Table 19 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(NBG318S LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the NBG318S'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 39 Wizard Step 3: WAN MAC Address



The following table describes the fields in this screen.

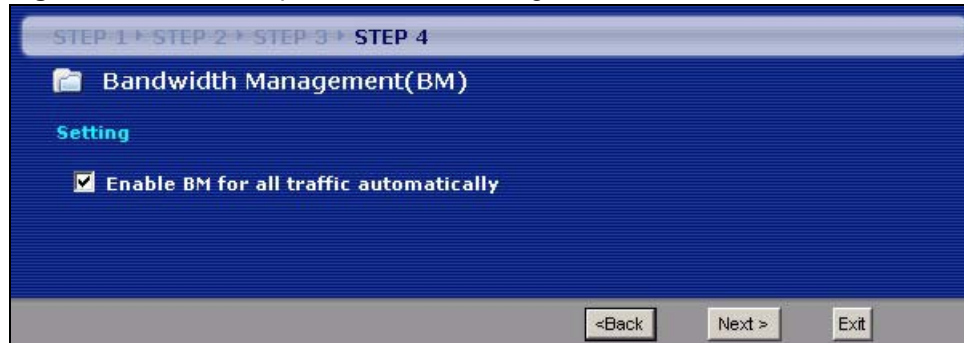
Table 20 Wizard Step 3: WAN MAC Address

LABEL	DESCRIPTION
Factory Default	Select Factory Default 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 Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit 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 NBG318S'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 40 Wizard Step 4: Bandwidth Management



The following fields describe the label in this screen.

Table 21 Wizard Step 4: Bandwidth Management

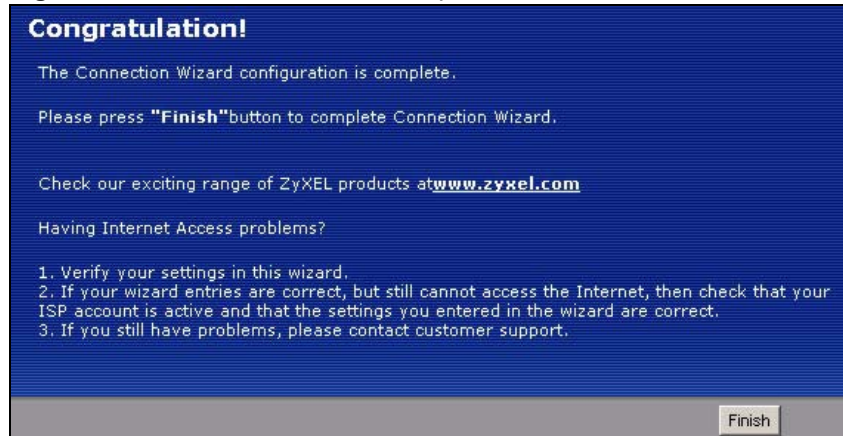
LABEL	DESCRIPTION
Enable BM for all traffic automatically	Select the check box to have the NBG318S apply bandwidth management to traffic going out through the NBG318S's WAN, LAN, HomePlug AV or WLAN port. Bandwidth is allocated according to the traffic type automatically. Real-time packets, such as VoIP traffic always get higher priority.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

4.6 Connection Wizard Complete

Click **Apply** to save your configuration.

Figure 41 Connection Wizard Save

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

Figure 42 Connection Wizard Complete

Well done! You have successfully set up your NBG318S to operate on your network and access the Internet.

PART II

Network

Wireless LAN (73)

WAN (93)

LAN (103)

HomePlug AV (109)

DHCP (115)

Network Address Translation (NAT) (119)

Dynamic DNS (129)

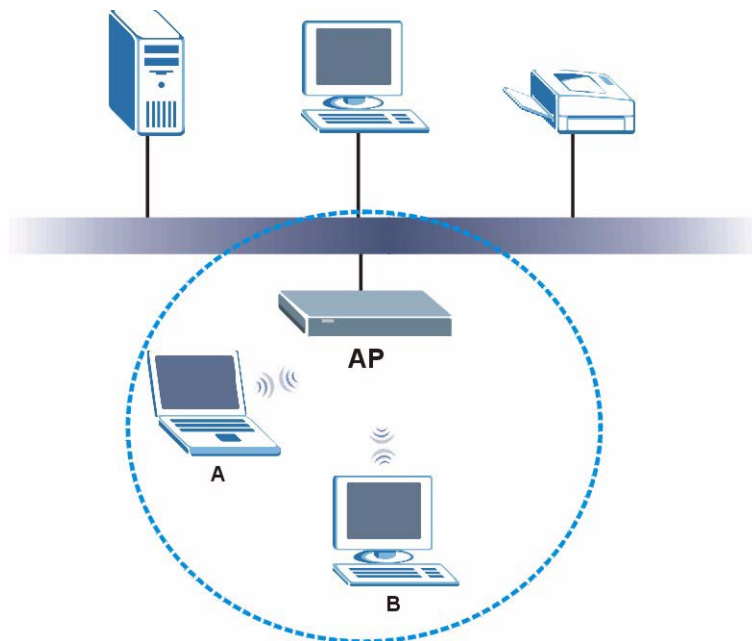
Wireless LAN

This chapter discusses how to configure the wireless network settings in your NBG318S. 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 43 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 NBG318S 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.

Requirements

To add a wireless LAN to your existing network, make sure you have the following:

- 1 an access point (AP) or a router with the wireless feature
- 2 at least one wireless network card/adaptor which varies according to your computer.
 - If you have a desktop, use either a wireless USB adapter or a wireless PCI adapter.
 - If you have a laptop, use either a wireless USB adapter or a wireless CardBus card.
- 3 a RADIUS server only if you want to use IEEE802.1x, WPA or WPA2

To have two or more computers communicate with each other wirelessly without an AP or wireless router, make sure you have the following:

- 1 two or more wireless network cards/adaptors which vary according to your computers.
 - If you have a desktop, use either a wireless USB adapter or a wireless PCI adapter.
 - If you have a laptop, use either a wireless USB adapter or a wireless CardBus card.

Setup Information

To set up your wireless network using an AP or wireless router, make sure your AP or wireless router and wireless network card(s)/adaptor(s) use the same following settings:

- SSID: _____
- Channel: auto or _____
- Network type of a wireless network card/adaptor: Infrastructure
- wireless standard: IEEE 802.11b, g, b/g or a
- Security:
 - () None
 - () WEP (64bit, 128bit or 256bit key) (ASCII or Hex): _____
 - () IEEE 802.1x
 - () WPA-PSK (TKIP or AES): _____
 - () WPA (TKIP or AES)
 - () WPA2-PSK (TKIP or AES): _____

WPA2 (TKIP or AES)

- Preamble type (if available): auto, short or long

To set up your wireless network without an AP or wireless router, make sure wireless network cards/adapters use the same following settings:

- Network type: Ad-Hoc
- SSID: _____
- Channel: _____
- wireless standard: IEEE 802.11b, g, b/g or a
- Security:
 - None
 - WEP (64bit, 128bit or 256bit key) (ASCII or Hex): _____

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.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each 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.

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.

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.

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 76](#) for information about this.)

Table 22 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest  Strongest	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 NBG318S, 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 NBG318S.

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 Roaming

A wireless station is a device with an IEEE 802.11a/b/g compliant wireless interface. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

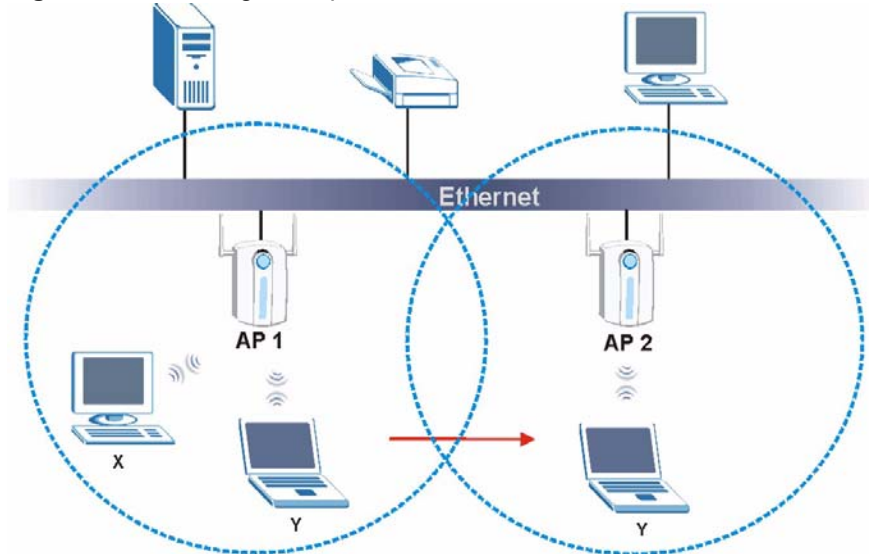
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is known as roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the other access points on the LAN about the change. An example is shown in [Figure 44 on page 78](#).

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this). 802.1x authentication information is not exchanged (at the time of writing).

Figure 44 Roaming Example



The steps below describe the roaming process.

- 1 Wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**.
- 2 Wireless station **Y** scans and detects the signal of access point **AP 2**.
- 3 Wireless station **Y** sends an association request to access point **AP 2**.
- 4 Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.
- 5 Access point **AP 1** updates the new position of wireless station **Y**.

5.3.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

- 1 All the access points must be on the same subnet and configured with the same ESSID.
- 2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
- 3 The adjacent access points should use different radio channels when their coverage areas overlap.
- 4 All access points must use the same port number to relay roaming information.
- 5 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

5.4 Quality of Service

This section discusses the Quality of Service (QoS) features available on the NBG318S.

5.4.1 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 NBG318S uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q tag or DSCP information in each packet's header. The NBG318S 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).

5.4.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the NBG318S uses.

Table 23 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.

5.5 General Wireless LAN Screen



If you are configuring the NBG318S from a computer connected to the wireless LAN and you change the NBG318S'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 NBG318S's new settings.

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

Figure 45 Network > Wireless LAN > General

The screenshot shows the 'General' configuration page for the wireless LAN. It includes sections for 'Wireless Setup' and 'Security'. In the 'Wireless Setup' section, the 'Enable Wireless LAN' checkbox is checked. The 'Name(SSID)' field contains 'ZyXEL'. The 'Hide SSID' checkbox is unchecked. The 'Channel Selection' dropdown is set to 'Channel-01 2412MHz', and the 'Operating Channel' is 'Channel-006'. In the 'Security' section, the 'Security Mode' dropdown is set to 'No Security'. At the bottom of the page, there are 'Apply' and 'Reset' buttons.

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

Table 24 Network > Wireless LAN > 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 NBG318S is currently using.
Apply	Click Apply to save your changes back to the NBG318S.
Reset	Click Reset to reload the previous configuration for this screen.

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

5.5.1 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 NBG318S, your network is accessible to any wireless networking device that is within range.