

NBG420N

Wireless N Router

DRAFT

User's Guide

Version 3.60

3/2008

Edition 1

DEFAULT LOGIN

IP Address <http://192.168.1.1>

Password 1234

DRAFT

ZyXEL
www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NBG420N 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 NBG420N.

- 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 NBG420N may be referred to as the “NBG420N”, 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 NBG420N icon is not an exact representation of your device.

NBG420N 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 
Modem 		

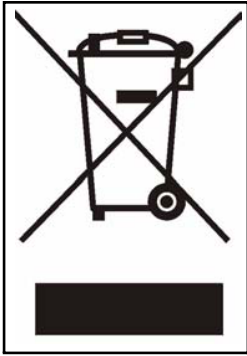
Safety Warnings



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.



DRAFT

Contents Overview

Introduction	29
Getting to Know Your NBG420N	31
The WPS Button	35
Introducing the Web Configurator	37
Connection Wizard	49
AP Mode	65
Tutorials	73
Network	87
Wireless LAN	89
WAN	117
LAN	127
DHCP	133
Network Address Translation (NAT)	137
Dynamic DNS	147
Security	151
Firewall	153
Content Filtering	161
IPSec VPN	165
Management	193
Static Route Screens	195
Bandwidth Management	199
Remote Management	209
Universal Plug-and-Play (UPnP)	215
Maintenance and Troubleshooting	227
System	229
Logs	233
Tools	251
Configuration Mode	257
Sys Op Mode	259
Language	263
Troubleshooting	265
Appendices and Index	271

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 NBG420N.....	31
1.1 Overview	31
1.2 Router Mode	31
1.3 AP Mode	32
1.4 Router Features vs. AP Features	32
1.5 Ways to Manage the NBG420N	33
1.6 Good Habits for Managing the NBG420N	33
1.7 LEDs	33
Chapter 2	
The WPS Button.....	35
2.1 Overview	35
Chapter 3	
Introducing the Web Configurator	37
3.1 Web Configurator Overview	37
3.2 Accessing the Web Configurator	37
3.3 Resetting the NBG420N	39
3.3.1 Procedure to Use the Reset Button	39
3.4 Navigating the Web Configurator	39
3.5 The Status Screen in Router Mode	39
3.5.1 Navigation Panel	42

3.5.2 Summary: Any IP Table	44
3.5.3 Summary: Bandwidth Management Monitor	44
3.5.4 Summary: DHCP Table	45
3.5.5 Summary: Packet Statistics	46
3.5.6 Summary: VPN Monitor	47
3.5.7 Summary: Wireless Station Status	47
Chapter 4	
Connection Wizard	49
4.1 Wizard Setup	49
4.2 Connection Wizard: STEP 1: System Information	50
4.2.1 System Name	50
4.2.2 Domain Name	51
4.3 Connection Wizard: STEP 2: Wireless LAN	51
4.3.1 Basic (WEP) Security	53
4.3.2 Extend (WPA-PSK or WPA2-PSK) Security	54
4.4 Connection Wizard: STEP 3: Internet Configuration	54
4.4.1 Ethernet Connection	55
4.4.2 PPPoE Connection	55
4.4.3 PPTP Connection	56
4.4.4 Your IP Address	58
4.4.5 WAN IP Address Assignment	58
4.4.6 IP Address and Subnet Mask	59
4.4.7 DNS Server Address Assignment	59
4.4.8 WAN IP and DNS Server Address Assignment	60
4.4.9 WAN MAC Address	61
4.5 Connection Wizard: STEP 4: Bandwidth management	62
4.6 Connection Wizard Complete	62
Chapter 5	
AP Mode.....	65
5.1 AP Mode Overview	65
5.2 Setting your NBG420N to AP Mode	65
5.3 The Status Screen in AP Mode	66
5.3.1 Navigation Panel	68
5.4 Configuring Your Settings	69
5.4.1 LAN Settings	69
5.4.2 WLAN and Maintenance Settings	71
5.5 Logging in to the Web Configurator in AP Mode	71
Chapter 6	
Tutorials	73
6.1 Wireless Tutorials	73

6.1.1 How to Connect to the Internet from an AP	73
6.1.2 Configure Wireless Security Using WPS on both your NBG420N and Wireless Client	73
6.1.3 Enable and Configure Wireless Security without WPS on your NBG420N	76
6.1.4 Configure Your Notebook	78
6.2 Site-To-Site VPN Tunnel Tutorial	80
6.2.1 Configuring Bob's NBG420N VPN Settings	81
6.2.2 Configuring Jack's NBG420N VPN Settings	83
6.2.3 Checking the VPN Connection	84
Part II: Network.....	87
Chapter 7	
Wireless LAN.....	89
7.1 Wireless Network Overview	89
7.2 Wireless Security Overview	90
7.2.1 SSID	90
7.2.2 MAC Address Filter	90
7.2.3 User Authentication	90
7.2.4 Encryption	91
7.3 Roaming	92
7.3.1 Requirements for Roaming	93
7.4 Quality of Service	93
7.4.1 WMM QoS	94
7.5 General Wireless LAN Screen	94
7.5.1 No Security	96
7.5.2 WEP Encryption	96
7.5.3 WPA-PSK/WPA2-PSK	98
7.5.4 WPA/WPA2	99
7.6 MAC Filter	101
7.7 Wireless LAN Advanced Screen	102
7.8 Quality of Service (QoS) Screen	103
7.8.1 Application Priority Configuration	105
7.9 WiFi Protected Setup	106
7.9.1 WPS Screen	106
7.9.2 WPS Station Screen	107
7.9.3 Scheduling	107
7.10 iPod Touch Web Configurator	108
7.10.1 Login Screen	109
7.10.2 System Status	110
7.10.3 WPS in Progress	112
7.10.4 Port Forwarding	113

7.11 Accessing the iPod Touch Web Configurator	114
7.11.1 Accessing the iPod Touch Web Configurator	115
Chapter 8	
WAN.....	117
8.1 WAN Overview	117
8.2 WAN MAC Address	117
8.3 Multicast	117
8.4 Internet Connection	118
8.4.1 Ethernet Encapsulation	118
8.4.2 PPPoE Encapsulation	119
8.4.3 PPTP Encapsulation	122
8.5 Advanced WAN Screen	125
Chapter 9	
LAN.....	127
9.1 LAN Overview	127
9.1.1 IP Pool Setup	127
9.1.2 System DNS Servers	127
9.2 LAN TCP/IP	127
9.2.1 Factory LAN Defaults	127
9.2.2 IP Address and Subnet Mask	128
9.2.3 Multicast	128
9.2.4 Any IP	128
9.3 LAN IP Screen	130
9.4 LAN IP Alias	130
9.5 Advanced LAN Screen	131
Chapter 10	
DHCP.....	133
10.1 DHCP	133
10.2 DHCP General Screen	133
10.3 DHCP Advanced Screen	134
10.4 Client List Screen	135
Chapter 11	
Network Address Translation (NAT).....	137
11.1 NAT Overview	137
11.2 Using NAT	137
11.2.1 Port Forwarding: Services and Port Numbers	137
11.2.2 Configuring Servers Behind Port Forwarding Example	138
11.3 General NAT Screen	138
11.4 NAT Application Screen	139

11.4.1 Game List Example	141
11.5 Trigger Port Forwarding	142
11.5.1 Trigger Port Forwarding Example	142
11.5.2 Two Points To Remember About Trigger Ports	143
11.6 NAT Advanced Screen	143
Chapter 12	
Dynamic DNS	147
12.1 Dynamic DNS Introduction	147
12.1.1 DynDNS Wildcard	147
12.2 Dynamic DNS Screen	147
Part III: Security.....	151
Chapter 13	
Firewall.....	153
13.1 Introduction to ZyXEL's Firewall	153
13.1.1 What is a Firewall?	153
13.1.2 Stateful Inspection Firewall	153
13.1.3 About the NBG420N Firewall	153
13.1.4 Guidelines For Enhancing Security With Your Firewall	154
13.2 Triangle Routes	154
13.2.1 Triangle Routes and IP Alias	154
13.3 General Firewall Screen	155
13.4 Services Screen	156
13.4.1 The Add Firewall Rule Screen	157
Chapter 14	
Content Filtering	161
14.1 Introduction to Content Filtering	161
14.2 Restrict Web Features	161
14.3 Days and Times	161
14.4 Filter Screen	161
14.5 Schedule	163
14.6 Customizing Keyword Blocking URL Checking	164
14.6.1 Domain Name or IP Address URL Checking	164
14.6.2 Full Path URL Checking	164
14.6.3 File Name URL Checking	164
Chapter 15	
IPSec VPN.....	165

15.1 IPSec VPN Overview	165
15.1.1 What You Can Do in the IPSec VPN Screens	165
15.1.2 What You Need To Know About IPSec VPN	166
15.1.3 IKE SA (IKE Phase 1) Overview	166
15.1.4 IPSec SA (IKE Phase 2) Overview	167
15.2 The General Screen	167
15.2.1 VPN Rule Setup (Basic)	168
15.2.2 VPN Rule Setup (Advanced)	173
15.2.3 VPN Rule Setup (Manual)	179
15.3 The SA Monitor Screen	183
15.4 VPN and Remote Management	184
15.5 IPSec VPN Technical Reference	185
Part IV: Management.....	193
Chapter 16	
Static Route Screens	195
16.1 Static Route Overview	195
16.2 IP Static Route Screen	195
16.2.1 Static Route Setup Screen	196
Chapter 17	
Bandwidth Management.....	199
17.1 Bandwidth Management Overview	199
17.2 Application-based Bandwidth Management	199
17.3 Subnet-based Bandwidth Management	199
17.4 Application and Subnet-based Bandwidth Management	200
17.5 Bandwidth Management Priorities	200
17.6 Predefined Bandwidth Management Services	201
17.6.1 Services and Port Numbers	201
17.7 Default Bandwidth Management Classes and Priorities	202
17.8 Bandwidth Management General Configuration	202
17.9 Bandwidth Management Advanced Configuration	203
17.9.1 Rule Configuration with the Pre-defined Service	205
17.9.2 Rule Configuration: User Defined Service Rule Configuration	205
17.10 Bandwidth Management Monitor	206
Chapter 18	
Remote Management.....	209
18.1 Remote Management Overview	209
18.1.1 Remote Management Limitations	209

18.1.2 Remote Management and NAT	210
18.1.3 System Timeout	210
18.2 WWW Screen	210
18.3 Telnet	211
18.4 Telnet Screen	211
18.5 FTP Screen	212
18.6 DNS Screen	212
Chapter 19	
Universal Plug-and-Play (UPnP).....	215
19.1 Introducing Universal Plug and Play	215
19.1.1 How do I know if I'm using UPnP?	215
19.1.2 NAT Traversal	215
19.1.3 Cautions with UPnP	215
19.2 UPnP and ZyXEL	216
19.3 UPnP Screen	216
19.4 Installing UPnP in Windows Example	217
Part V: Maintenance and Troubleshooting	227
Chapter 20	
System	229
20.1 System Overview	229
20.2 System General Screen	229
20.3 Time Setting Screen	230
Chapter 21	
Logs	233
21.1 View Log	233
21.2 Log Settings	234
21.3 Log Descriptions	237
Chapter 22	
Tools.....	251
22.1 Firmware Upload Screen	251
22.2 Configuration Screen	252
22.2.1 Backup Configuration	253
22.2.2 Restore Configuration	253
22.2.3 Back to Factory Defaults	254
22.3 Restart Screen	254
22.4 Wake On LAN	255

Chapter 23	
Configuration Mode	257
Chapter 24	
Sys Op Mode	259
24.1 Overview	259
24.1.1 Router	259
24.1.2 AP	259
24.2 Selecting System Operation Mode	260
Chapter 25	
Language	263
25.1 Language Screen	263
Chapter 26	
Troubleshooting	265
26.1 Power, Hardware Connections, and LEDs	265
26.2 NBG420N Access and Login	266
26.3 Internet Access	268
26.4 Resetting the NBG420N to Its Factory Defaults	269
26.5 Wireless Router/AP Troubleshooting	269
26.6 Advanced Features	270
Part VI: Appendices and Index	271
Appendix A Product Specifications and Wall-Mounting Instructions	273
Appendix B Pop-up Windows, JavaScripts and Java Permissions	279
Appendix C IP Addresses and Subnetting	285
Appendix D Setting up Your Computer's IP Address	293
26.6.1 Verifying Settings	308
Appendix E Wireless LANs	309
26.6.2 WPA(2)-PSK Application Example	318
26.6.3 WPA(2) with RADIUS Application Example	318
Appendix F Services	321
Appendix G Legal Information	325
Appendix H Customer Support	329
Index	335

List of Figures

Figure 1 Secure Wireless Internet Access in Router Mode	31
Figure 2 Wireless Internet Access in AP Mode	32
Figure 3 Front Panel	33
Figure 4 Change Password Screen	38
Figure 5 Selecting the setup mode	39
Figure 6 Web Configurator Status Screen	40
Figure 7 Any IP Table	44
Figure 8 Summary: BW MGMT Monitor	45
Figure 9 Summary: DHCP Table	45
Figure 10 Summary: Packet Statistics	46
Figure 11 Summary: VPN Monitor	47
Figure 12 Summary: Wireless Association List	47
Figure 13 Select Wizard or Advanced Mode	49
Figure 14 Select a Language	50
Figure 15 Welcome to the Connection Wizard	50
Figure 16 Wizard Step 1: System Information	51
Figure 17 Wizard Step 2: Wireless LAN	52
Figure 18 Wizard Step 2: Basic (WEP) Security	53
Figure 19 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security	54
Figure 20 Wizard Step 3: ISP Parameters	55
Figure 21 Wizard Step 3: Ethernet Connection	55
Figure 22 Wizard Step 3: PPPoE Connection	56
Figure 23 Wizard Step 3: PPTP Connection	57
Figure 24 Wizard Step 3: Your IP Address	58
Figure 25 Wizard Step 3: WAN IP and DNS Server Addresses	60
Figure 26 Wizard Step 3: WAN MAC Address	61
Figure 27 Wizard Step 4: Bandwidth Management	62
Figure 28 Connection Wizard Save	63
Figure 29 Connection Wizard Complete	63
Figure 30 Wireless Internet Access in AP Mode	65
Figure 31 Maintenance > Sys OP Mode > General	66
Figure 32 Status: AP Mode	66
Figure 33 Menu: AP Mode	68
Figure 34 Network > LAN > IP	70
Figure 35 Wireless AP Connection to the Internet	73
Figure 36 Example WPS Process: PBC Method	75
Figure 37 Example WPS Process: PIN Method	76
Figure 38 Network > Wireless LAN > General	77

Figure 39 Status: AP Mode	78
Figure 40 Connecting a Wireless Client to a Wireless Network t	79
Figure 41 Security Settings	79
Figure 42 Confirm Save	79
Figure 43 Link Status	80
Figure 44 Site-To-Site VPN Tunnel	80
Figure 45 Property	81
Figure 46 Local Policy	81
Figure 47 Remote Policy	82
Figure 48 Authentication Method	82
Figure 49 IPsec Algorithm	82
Figure 50 VPN Summary	83
Figure 51 Property	83
Figure 52 Local Policy	83
Figure 53 Remote Policy	83
Figure 54 Authentication Method	84
Figure 55 IPsec Algorithm	84
Figure 56 VPN Summary	84
Figure 57 Pinging Jack's Local IP Address	85
Figure 58 SA Monitor	85
Figure 59 Example of a Wireless Network	89
Figure 60 Roaming Example	93
Figure 61 Network > Wireless LAN > General	95
Figure 62 Network > Wireless LAN > General: No Security	96
Figure 63 Network > Wireless LAN > General: Static WEP	97
Figure 64 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK	98
Figure 65 Network > Wireless LAN > General: WPA/WPA2	100
Figure 66 Network > Wireless LAN > MAC Filter	102
Figure 67 Network > Wireless LAN > Advanced	103
Figure 68 Network > Wireless LAN > QoS	104
Figure 69 Network > Wireless LAN > QoS: Application Priority Configuration	105
Figure 70 WPS	106
Figure 71 WPS Station	107
Figure 72 Scheduling	108
Figure 73 Login Screen	109
Figure 74 System Status screen	111
Figure 75 WPS In Progress	113
Figure 76 Port Forwarding	114
Figure 77 Login Screen	115
Figure 78 Network > WAN > Internet Connection: Ethernet Encapsulation	118
Figure 79 Network > WAN > Internet Connection: PPPoE Encapsulation	120
Figure 80 Network > WAN > Internet Connection: PPTP Encapsulation	123
Figure 81 Network > WAN > Advanced	125

Figure 82 Any IP Example	129
Figure 83 Network > LAN > IP	130
Figure 84 Network > LAN > IP Alias	131
Figure 85 Network > LAN > Advanced	131
Figure 86 Network > DHCP > General	133
Figure 87 Network > DHCP > Advanced	134
Figure 88 Network > DHCP > Client List	136
Figure 89 Multiple Servers Behind NAT Example	138
Figure 90 Network > NAT > General	138
Figure 91 Network > NAT > Application	140
Figure 92 Game List Example	142
Figure 93 Trigger Port Forwarding Process: Example	143
Figure 94 Network > NAT > Advanced	144
Figure 95 Dynamic DNS	148
Figure 96 Using IP Alias to Solve the Triangle Route Problem	155
Figure 97 Security > Firewall > General I	155
Figure 98 Security > Firewall > Services	156
Figure 99 Security > Firewall > Services > Adding a Rule	158
Figure 100 Security > Content Filter > Filter	162
Figure 101 Security > Content Filter > Schedule	163
Figure 102 IPSec VPN: Overview	165
Figure 103 VPN: IKE SA and IPSec SA	166
Figure 104 Security > VPN > General	167
Figure 105 IPSec Fields Summary	169
Figure 106 Security > VPN > General > Rule Setup: IKE (Basic)	169
Figure 107 Security > VPN > General > Rule Setup: IKE (Advanced)	174
Figure 108 Security > VPN > General > Rule Setup: Manual	180
Figure 109 Security > VPN > SA Monitor	183
Figure 110 VPN for Remote Management Example	184
Figure 111 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal	185
Figure 112 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange	185
Figure 113 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication	186
Figure 114 VPN/NAT Example	188
Figure 115 VPN: Transport and Tunnel Mode Encapsulation	189
Figure 116 Private DNS Server Example	191
Figure 117 Example of Static Routing Topology	195
Figure 118 Management > Static Route > IP Static Route	196
Figure 119 Management > Static Route > IP Static Route: Static Route Setup	197
Figure 120 Subnet-based Bandwidth Management Example	200
Figure 121 Management > Bandwidth MGMT > General	202
Figure 122 Management > Bandwidth MGMT > Advanced	203
Figure 123 Bandwidth Management Rule Configuration: Pre-defined Service	205
Figure 124 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration	206

Figure 125 Management > Bandwidth MGMT > Monitor	207
Figure 126 Management > Remote MGMT > WWW	210
Figure 127 Management > Remote MGMT > Telnet	211
Figure 128 Management > Remote MGMT > FTP	212
Figure 129 Management > Remote MGMT > DNS	213
Figure 130 Management > UPnP > General	216
Figure 131 Add/Remove Programs: Windows Setup: Communication	217
Figure 132 Add/Remove Programs: Windows Setup: Communication: Components	218
Figure 133 Network Connections	218
Figure 134 Windows Optional Networking Components Wizard	219
Figure 135 Networking Services	219
Figure 136 Network Connections	220
Figure 137 Internet Connection Properties	221
Figure 138 Internet Connection Properties: Advanced Settings	222
Figure 139 Internet Connection Properties: Advanced Settings: Add	222
Figure 140 System Tray Icon	223
Figure 141 Internet Connection Status	223
Figure 142 Network Connections	224
Figure 143 Network Connections: My Network Places	225
Figure 144 Network Connections: My Network Places: Properties: Example	225
Figure 145 Maintenance > System > General	229
Figure 146 Maintenance > System > Time Setting	230
Figure 147 Maintenance > Logs > View Log	233
Figure 148 Maintenance > Logs > Log Settings	235
Figure 149 Maintenance > Tools > Firmware	251
Figure 150 Upload Warning	252
Figure 151 Network Temporarily Disconnected	252
Figure 152 Upload Error Message	252
Figure 153 Maintenance > Tools > Configuration	253
Figure 154 Configuration Restore Successful	254
Figure 155 Temporarily Disconnected	254
Figure 156 Configuration Restore Error	254
Figure 157 Maintenance > Tools > Restart	255
Figure 158 Maintenance > Tools > Wake On LAN	255
Figure 159 Maintenance > Config Mode > General	257
Figure 160 LAN and WAN IP Addresses in Router Mode	259
Figure 161 IP Address in AP Mode	260
Figure 162 Maintenance > Sys OP Mode > General	260
Figure 163 Maintenance > Sys Op Mode > General: Router	260
Figure 164 Maintenance > Sys Op Mode > General: AP	261
Figure 165 Language	263
Figure 166 Wall-mounting Example	277
Figure 167 Masonry Plug and M4 Tap Screw	278

Figure 168 Pop-up Blocker	279
Figure 169 Internet Options: Privacy	280
Figure 170 Internet Options: Privacy	281
Figure 171 Pop-up Blocker Settings	281
Figure 172 Internet Options: Security	282
Figure 173 Security Settings - Java Scripting	283
Figure 174 Security Settings - Java	283
Figure 175 Java (Sun)	284
Figure 176 Network Number and Host ID	286
Figure 177 Subnetting Example: Before Subnetting	288
Figure 178 Subnetting Example: After Subnetting	289
Figure 179 WIndows 95/98/Me: Network: Configuration	294
Figure 180 Windows 95/98/Me: TCP/IP Properties: IP Address	295
Figure 181 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	296
Figure 182 Windows XP: Start Menu	297
Figure 183 Windows XP: Control Panel	297
Figure 184 Windows XP: Control Panel: Network Connections: Properties	298
Figure 185 Windows XP: Local Area Connection Properties	298
Figure 186 Windows XP: Internet Protocol (TCP/IP) Properties	299
Figure 187 Windows XP: Advanced TCP/IP Properties	300
Figure 188 Windows XP: Internet Protocol (TCP/IP) Properties	301
Figure 189 Macintosh OS 8/9: Apple Menu	302
Figure 190 Macintosh OS 8/9: TCP/IP	302
Figure 191 Macintosh OS X: Apple Menu	303
Figure 192 Macintosh OS X: Network	304
Figure 193 Red Hat 9.0: KDE: Network Configuration: Devices	305
Figure 194 Red Hat 9.0: KDE: Ethernet Device: General	306
Figure 195 Red Hat 9.0: KDE: Network Configuration: DNS	306
Figure 196 Red Hat 9.0: KDE: Network Configuration: Activate	307
Figure 197 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	307
Figure 198 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	307
Figure 199 Red Hat 9.0: DNS Settings in resolv.conf	308
Figure 200 Red Hat 9.0: Restart Ethernet Card	308
Figure 201 Red Hat 9.0: Checking TCP/IP Properties	308
Figure 202 Peer-to-Peer Communication in an Ad-hoc Network	309
Figure 203 Basic Service Set	310
Figure 204 Infrastructure WLAN	311
Figure 205 RTS/CTS	312
Figure 206 WPA(2)-PSK Authentication	318

List of Tables

Table 1 Features Available in Router Mode vs. AP Mode	32
Table 2 Front Panel LEDs	33
Table 3 Status Screen Icon Key	40
Table 4 Web Configurator Status Screen	40
Table 5 Screens Summary	42
Table 6 Summary: DHCP Table	45
Table 7 Summary: Packet Statistics	46
Table 8 Summary: Wireless Association List	47
Table 9 Summary: Wireless Association List	48
Table 10 Wizard Step 1: System Information	51
Table 11 Wizard Step 2: Wireless LAN	52
Table 12 Wizard Step 2: Basic (WEP) Security	53
Table 13 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security	54
Table 14 Wizard Step 3: ISP Parameters	55
Table 15 Wizard Step 3: PPPoE Connection	56
Table 16 Wizard Step 3: PPTP Connection	57
Table 17 Wizard Step 3: Your IP Address	58
Table 18 Private IP Address Ranges	58
Table 19 Wizard Step 3: WAN IP and DNS Server Addresses	60
Table 20 Example of Network Properties for LAN Servers with Fixed IP Addresses	61
Table 21 Wizard Step 3: WAN MAC Address	61
Table 22 Wizard Step 4: Bandwidth Management	62
Table 23 Web Configurator Status Screen	67
Table 24 Screens Summary	68
Table 25 Network > LAN > IP	70
Table 26 Site-To-Site VPN Tunnel Settings	80
Table 27 Types of Encryption for Each Type of Authentication	91
Table 28 WMM QoS Priorities	94
Table 29 Network > Wireless LAN > General	95
Table 30 Wireless No Security	96
Table 31 Network > Wireless LAN > General: Static WEP	97
Table 32 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK	99
Table 33 Network > Wireless LAN > General: WPA/WPA2	100
Table 34 Network > Wireless LAN > MAC Filter	102
Table 35 Network > Wireless LAN > Advanced	103
Table 36 Network > Wireless LAN > QoS	104
Table 37 WPS	106
Table 38 WPS Station	107

Table 39 Scheduling	108
Table 40 Login Screen	109
Table 41 System Status screen	111
Table 42 Port Forwarding	114
Table 43 Network > WAN > Internet Connection: Ethernet Encapsulation	119
Table 44 Network > WAN > Internet Connection: PPPoE Encapsulation	121
Table 45 Network > WAN > Internet Connection: PPTP Encapsulation	123
Table 46 WAN > Advanced	125
Table 47 Network > LAN > IP	130
Table 48 Network > LAN > IP Alias	131
Table 49 Network > LAN > Advanced	132
Table 50 Network > DHCP > General	133
Table 51 Network > DHCP > Advanced	134
Table 52 Network > DHCP > Client List	136
Table 53 Network > NAT > General	139
Table 54 NAT Application	140
Table 55 Network > NAT > Advanced	144
Table 56 Dynamic DNS	148
Table 57 Security > Firewall > General	155
Table 58 Security > Firewall > Services	156
Table 59 Security > Firewall > Services > Adding a Rule	158
Table 60 Security > Content Filter > Filter	162
Table 61 Security > Content Filter > Schedule	163
Table 62 Security > VPN > General	168
Table 63 SECURITY > VPN > Rule Setup: IKE (Basic)	170
Table 64 Security > VPN > Rule Setup: IKE (Advanced)	175
Table 65 Security > VPN > Rule Setup: Manual	180
Table 66 Security > VPN > SA Monitor	184
Table 67 VPN Example: Matching ID Type and Content	186
Table 68 VPN Example: Mismatching ID Type and Content	187
Table 69 Management > Static Route > IP Static Route	196
Table 70 Management > Static Route > IP Static Route: Static Route Setup	197
Table 71 Application and Subnet-based Bandwidth Management Example	200
Table 72 Bandwidth Management Priorities	200
Table 73 Media Bandwidth Management Setup: Services	201
Table 74 Bandwidth Management Priority with Default Classes	202
Table 75 Management > Bandwidth MGMT > General	203
Table 76 Management > Bandwidth MGMT > Advanced	204
Table 77 Bandwidth Management Rule Configuration: Pre-defined Service	205
Table 78 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration ..	206
Table 79 Management > Remote MGMT > WWW	210
Table 80 Management > Remote MGMT > Telnet	211
Table 81 Management > Remote MGMT > FTP	212

Table 82 Management > Remote MGMT > DNS	213
Table 83 Management > UPnP > General	216
Table 84 Maintenance > System > General	229
Table 85 Maintenance > System > Time Setting	231
Table 86 Maintenance > Logs > View Log	234
Table 87 Maintenance > Logs > Log Settings	235
Table 88 System Maintenance Logs	237
Table 89 System Error Logs	238
Table 90 Access Control Logs	238
Table 91 TCP Reset Logs	238
Table 92 Packet Filter Logs	239
Table 93 ICMP Logs	239
Table 94 CDR Logs	240
Table 95 PPP Logs	240
Table 96 UPnP Logs	240
Table 97 Content Filtering Logs	240
Table 98 Attack Logs	241
Table 99 IPsec Logs	242
Table 100 IKE Logs	242
Table 101 PKI Logs	245
Table 102 802.1X Logs	246
Table 103 ACL Setting Notes	247
Table 104 ICMP Notes	247
Table 105 Syslog Logs	248
Table 106 RFC-2408 ISAKMP Payload Types	249
Table 107 Maintenance > Tools > Firmware	251
Table 108 Maintenance Restore Configuration	253
Table 109 Maintenance > Tools > Wake On LAN	255
Table 110 Maintenance > Config Mode > General	257
Table 111 Advanced Configuration Options	258
Table 112 Maintenance > Sys OP Mode > General	261
Table 113 Hardware Features	273
Table 114 Firmware Features	274
Table 115 Feature Specifications	275
Table 116 Standards Supported	276
Table 117 Subnet Mask - Identifying Network Number	286
Table 118 Subnet Masks	287
Table 119 Maximum Host Numbers	287
Table 120 Alternative Subnet Mask Notation	287
Table 121 Subnet 1	289
Table 122 Subnet 2	290
Table 123 Subnet 3	290
Table 124 Subnet 4	290

List of Tables

Table 125 Eight Subnets	290
Table 126 24-bit Network Number Subnet Planning	291
Table 127 16-bit Network Number Subnet Planning	291
Table 128 IEEE 802.11g	313
Table 129 Comparison of EAP Authentication Types	316
Table 130 Wireless Security Relational Matrix	319
Table 131 Examples of Services	321

PART I

Introduction

Getting to Know Your NBG420N (31)

The WPS Button (35)

Introducing the Web Configurator (37)

Connection Wizard (49)

AP Mode (65)

Tutorials (73)

DRAFT

Getting to Know Your NBG420N

This chapter introduces the main features and applications of the NBG420N.

1.1 Overview

The NBG420N acts as either an access point (AP) or a secure broadband router for all data passing between the Internet and your local network. In both **AP** and **Router Mode** you can set up a wireless network with other IEEE 802.11b/g/n compatible devices. In **Router Mode** a number of services such as a firewall, IPSec VPN and content filtering are also available. You can use media bandwidth management to efficiently manage traffic on your network. Bandwidth management features allow you to prioritize time-sensitive or highly important applications such as Voice over the Internet (VoIP).

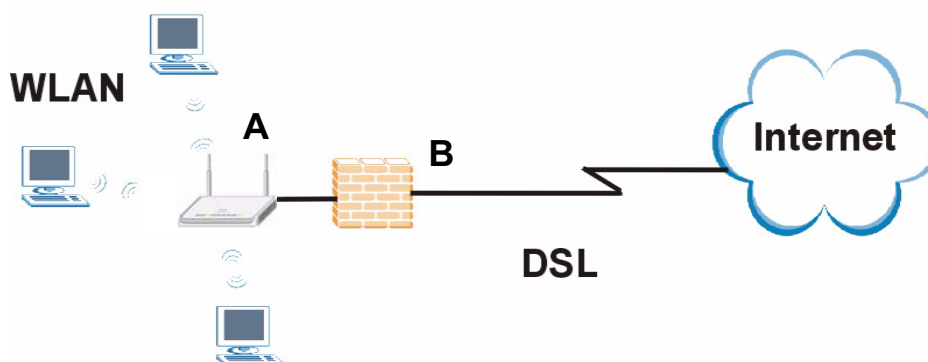
The NBG420N also uses MIMO (Multiple-In, Multiple-Out) antenna technology to deliver high-speed wireless networking.

1.2 Router Mode

Select **Router Mode** if you need to route traffic between your network and another network such as the Internet, and require important network services such as a firewall or bandwidth management.

The following figure shows computers in a WLAN connecting to the NBG420N (A), which has a DSL connection to the Internet. The NBG420N is set to **Router Mode** and has router features such as a built-in firewall (B).

Figure 1 Secure Wireless Internet Access in Router Mode

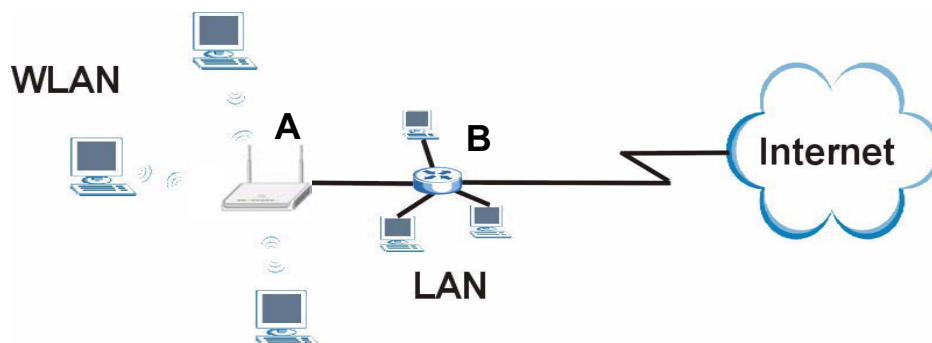


1.3 AP Mode

Select **AP Mode** if you already have a router or gateway on your network which provides network services such as a firewall or bandwidth management.

The following figure shows computers in a WLAN connecting to the NBG420N, which acts as an access point (**A**). The NBG420N allows the wireless computers to share the same Internet access as the other computers connected to the router (**B**) on the same network.

Figure 2 Wireless Internet Access in AP Mode



1.4 Router Features vs. AP Features

The following table shows which features are available in **Router** or **AP Mode**.

Table 1 Features Available in Router Mode vs. AP Mode

FEATURE	ROUTER MODE	AP MODE
DHCP This allows individual clients to obtain IP addresses at start-up from a DHCP server.	YES	NO
Firewall This establishes a network security barrier, protecting your network from attacks and controlling access between your network and the Internet.	YES	NO
Bandwidth Management This allows you to allocate network bandwidth to specific applications and or subnets.	YES	NO
Any IP This allows a computer to access the NBG420N when the IP addresses of the computer and the NBG420N are not in the same subnet.)	YES	NO
VPN A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines.	YES	NO
Wireless This allows two or more devices to communicate without wires, based on IEEE 802.11 wireless standards.	YES	YES

1.5 Ways to Manage the NBG420N

Use any of the following methods to manage the NBG420N.

- Web Configurator. This is recommended for everyday management of the NBG420N 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.

1.6 Good Habits for Managing the NBG420N

Do the following things regularly to make the NBG420N more secure and to manage the NBG420N 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 NBG420N to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG420N. You could simply restore your last configuration.

1.7 LEDs

Figure 3 Front Panel



The following table describes the LEDs.

Table 2 Front Panel LEDs






LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	The NBG420N is receiving power and functioning properly.
		Off	The NBG420N is not receiving power.

Table 2 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
LAN 1-4 	Green	On	The NBG420N has a successful 10MB Ethernet connection.
		Blinking	The NBG420N is sending/receiving data.
	Amber	On	The NBG420N has a successful 100MB Ethernet connection.
		Blinking	The NBG420N is sending/receiving data.
		Off	The LAN is not connected.
WAN 	Green	On	The NBG420N has a successful 10MB WAN connection.
		Blinking	The NBG420N is sending/receiving data.
	Amber	On	The NBG420N has a successful 100MB Ethernet connection.
		Blinking	The NBG420N is sending/receiving data.
		Off	The WAN connection is not ready, or has failed.
WLAN 	Green	On	The NBG420N is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG420N is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
WPS 	Green	On	WPS (WiFi Protected Setup) is configured on your device.
		Blinking	The NBG420N is attempting to connect with another wireless devices using WPS.
		Off	WPS is disabled on your device.

The WPS Button

2.1 Overview

Your NBG420N supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

For more information on using WPS, see [Section 6.1.2 on page 73](#).

Introducing the Web Configurator

This chapter describes how to access the NBG420N 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 NBG420N via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions or Safari 2.0 or 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 NBG420N hardware is properly connected and prepare your computer or computer network to connect to the NBG420N (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "http://192.168.1.1" as the website address.

Your computer must be in the same subnet in order to access this website address.

- In **Router Mode** enable the DHCP Server. The NBG420N assigns your computer an IP address on the same subnet.
- In **AP Mode** the NBG420N does not assign an IP address to your computer, so you should check it's in the same subnet. See [Section 5.5 on page 71](#) for more information.

- 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 4 Change Password Screen



ZyXEL

Please enter a new password

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

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

New Password:

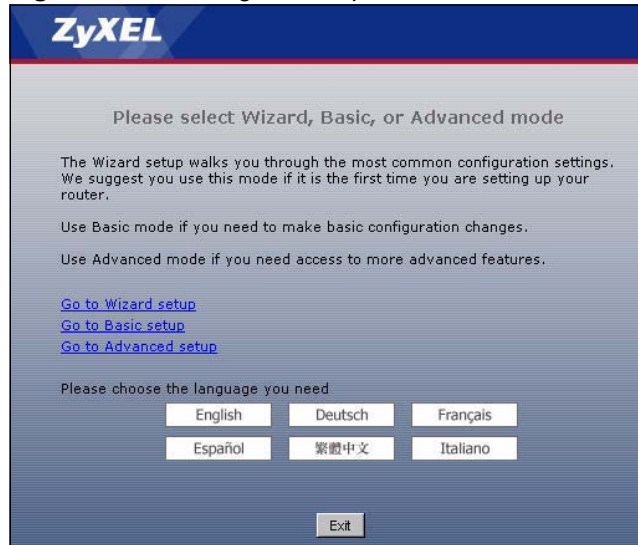
Retype to Confirm:

Apply Ignore



The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the NBG420N 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. See [Chapter 23 on page 257](#) for more information.
 - Click **Go to Advanced Setup** to view and configure all the NBG420N's settings.
 - Select a language to go to the basic web configurator in that language. To change to the advanced configurator see [Chapter 23 on page 257](#).

Figure 5 Selecting the setup mode

3.3 Resetting the NBG420N

If you forget your password or IP address, or you cannot access the web configurator, you will need to use the **RESET** button at the back of the NBG420N to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to “1234” and the IP address will be reset to “192.168.1.1”.

3.3.1 Procedure to Use the Reset Button

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for five seconds or until the power LED begins to blink and then release it. When the power LED begins to blink, the defaults have been restored and the NBG420N restarts.

3.4 Navigating the Web Configurator

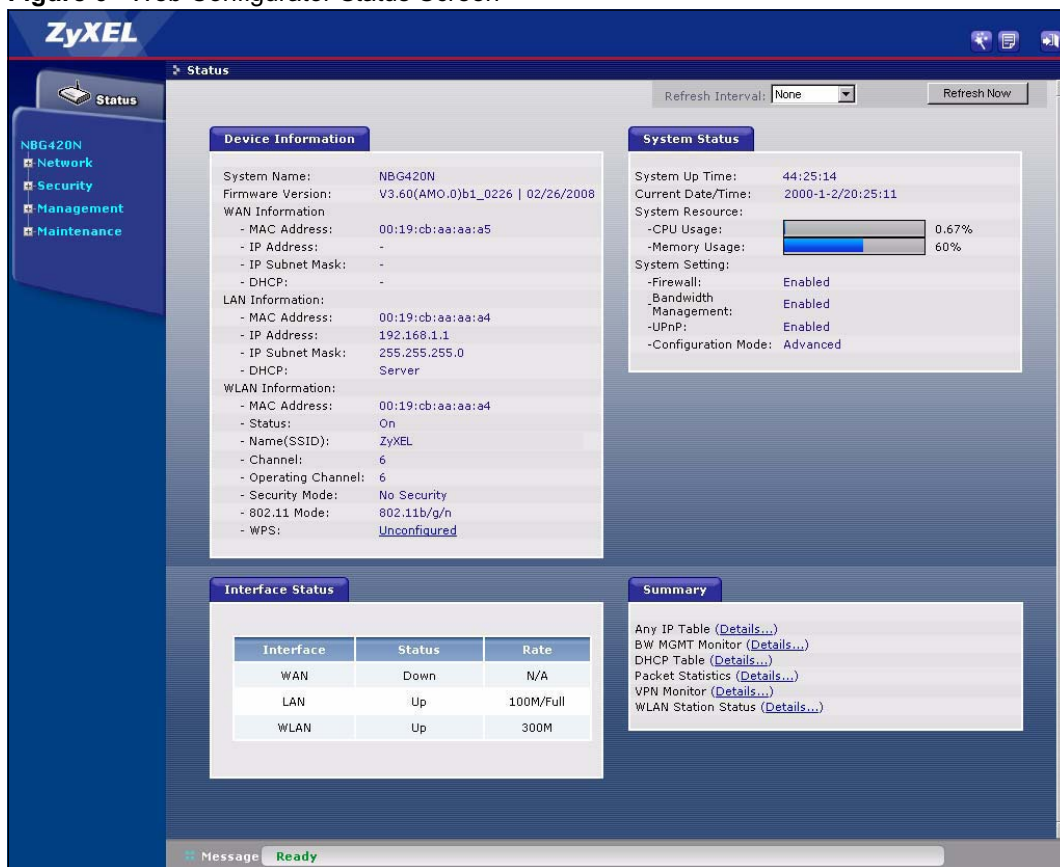
The following summarizes how to navigate the web configurator from the **Status** screen in **Router Mode** and **AP Mode**.

3.5 The Status Screen in Router Mode

Click on **Status**. The screen below shows the status screen in **Router Mode**.

(For information on the status screen in **AP Mode** see [Chapter 5 on page 66.](#))

Figure 6 Web Configurator Status Screen



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

Table 3 Status Screen Icon Key

ICON	DESCRIPTION
	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 4 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 firmware version and the date created.

Table 4 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
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.
- Status	This shows the current status of the Wireless LAN - On , Off or Off by scheduler .
- Name (SSID)	This shows a descriptive name used to identify the NBG420N in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG420N is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG420N is using.
- 802.11 Mode	This shows the wireless standard.
- WPS	This displays Configured when the WPS has been set up. This displays Unconfigured if the WPS has not been set up. Click the status to display Network > Wireless LAN > WPS screen.
System Status	
System Up Time	This is the total time the NBG420N has been on.
Current Date/Time	This field displays your NBG420N's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG420N's processing ability is currently used. When this percentage is close to 100%, the NBG420N 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 NBG420N is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall.
System Setting	
- Firewall	This shows whether the firewall is active or not.
- Bandwidth Management	This shows whether the bandwidth management is active or not.
- UPnP	This shows whether UPnP is active or not.
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (Advanced) or not (Basic).
Interface Status	
Interface	This displays the NBG420N port types. The port types are: WAN , LAN and WLAN .

Table 4 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
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.
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.
Summary	
Any IP Table	Use this screen to view details of IP addresses assigned to devices not in the same subnet as the NBG420N.
BW MGMT Monitor	Use this screen to view the NBG420N'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.
VPN Monitor	Use this screen to view the active VPN connections.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the NBG420N.

3.5.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG420N features.

The following table describes the sub-menus.

Table 5 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG420N's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG420N to block access to devices or block the devices from accessing the NBG420N.
	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.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
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.

Table 5 Screens Summary

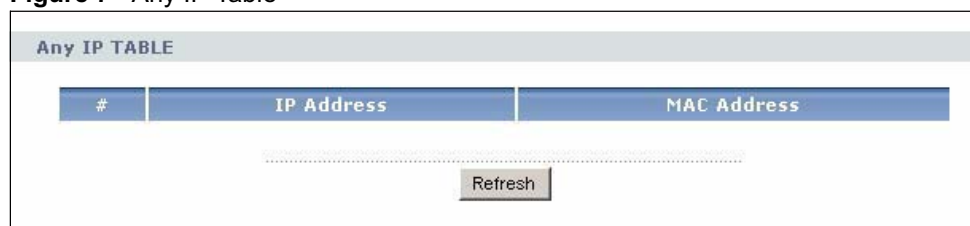
LINK	TAB	FUNCTION
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Advanced	Use this screen to enable other advanced properties.
DHCP Server	General	Use this screen to enable the NBG420N's DHCP server.
	Advanced	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 NBG420N.
	Advanced	Use this screen to change your NBG420N'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 NBG420N to perform content filtering.
VPN	General	Use this screen to configure VPN connections and view the rule summary.
	SA Monitor	Use this screen to display and manage active VPN connections.
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 NBG420N's bandwidth usage and allotments.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG420N.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG420N.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the NBG420N.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the NBG420N.
UPnP	General	Use this screen to enable UPnP on the NBG420N.
Maintenance		

Table 5 Screens Summary

LINK	TAB	FUNCTION
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 NBG420N'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 NBG420N's log settings.
Tools	Firmware	Use this screen to upload firmware to your NBG420N.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG420N.
	Restart	This screen allows you to reboot the NBG420N without turning the power off.
	Wake On LAN	Use this screen to remotely turn on a device on the network.
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 whether your device acts as a Router or a Access Point.
Language		This screen allows you to select the language you prefer.

3.5.2 Summary: Any IP Table

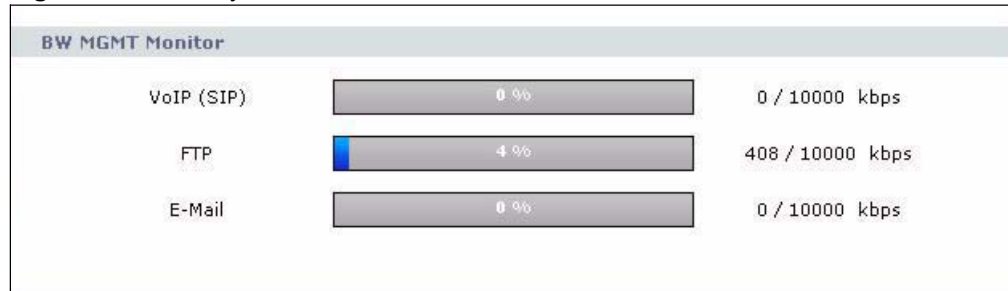
This screen displays the IP address of each computer that is using the NBG420N via the any IP feature. Any IP allows computers to access the Internet through the NBG420N without changing their network settings when NAT is enabled. To access this screen, open the **Status** screen (see [Section 3.5 on page 39](#)), and click (**Details...**) next to **Any IP Table**.

Figure 7 Any IP Table


Any IP TABLE		
#	IP Address	MAC Address
Refresh		

3.5.3 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 8 Summary: BW MGMT Monitor

3.5.4 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 NBG420N's LAN as a DHCP server or disable it. When configured as a server, the NBG420N provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, 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 NBG420N's DHCP server.

Figure 9 Summary: DHCP Table

DHCP Table			
#	IP Address	Host Name	MAC Address
1	192.168.1.33	TWPC12731	00:19:cb:04:80:1e
2	192.168.1.35	twpc12116	00:02:e3:56:16:9d

Refresh

The following table describes the labels in this screen.

Table 6 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the Host Name field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. 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.

3.5.5 Summary: Packet Statistics

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

Figure 10 Summary: Packet Statistics

Packet Statistics							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	68	296	0	0	0	00:00:00
LAN	100M/Full	12907	16373	0	774	583	1:01:02
WLAN	54M	4396	1022	0	0	0	5:52:58

System Up Time : 5:53:04

Poll Interval(s) : sec

The following table describes the labels in this screen.

Table 7 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG420N'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 NBG420N has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval(s) field.
Stop	Click Stop to stop refreshing statistics.

3.5.6 Summary: VPN Monitor

Click the **VPN Monitor (Details...)** hyperlink in the **Status** screen. This screen displays read-only information about the active VPN connections. Click the **Refresh** button to update the screen. A Security Association (SA) is the group of security settings related to a specific VPN tunnel.

Figure 11 Summary: VPN Monitor

The screenshot shows a web interface titled "Security Associations Table". Below the title is a sub-header "Current IPSec Security Associations". There is a table with four columns: "#", "Name", "Encapsulation", and "IPSec Algorithm". Below the table is a "Refresh" button.

#	Name	Encapsulation	IPSec Algorithm
Refresh			

The following table describes the labels in this screen.

Table 8 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN tunnel.
Encapsulation	This field displays Tunnel or Transport mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase NBG420N processing requirements and communications latency (delay).
Refresh	Click this button to update the screen's statistics immediately.

3.5.7 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 NBG420N in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 12 Summary: Wireless Association List

The screenshot shows a web interface titled "Association List". Below the title is a table with three columns: "#", "MAC Address", and "Association Time". The first row contains the values "001", "00:19:cb:04:80:1e", and "03:52:42 2000/01/01". Below the table is a "Refresh" button.

#	MAC Address	Association Time
001	00:19:cb:04:80:1e	03:52:42 2000/01/01
Refresh		

The following table describes the labels in this screen.

Table 9 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 NBG420N's WLAN network.
Refresh	Click Refresh to reload the list.

Connection Wizard

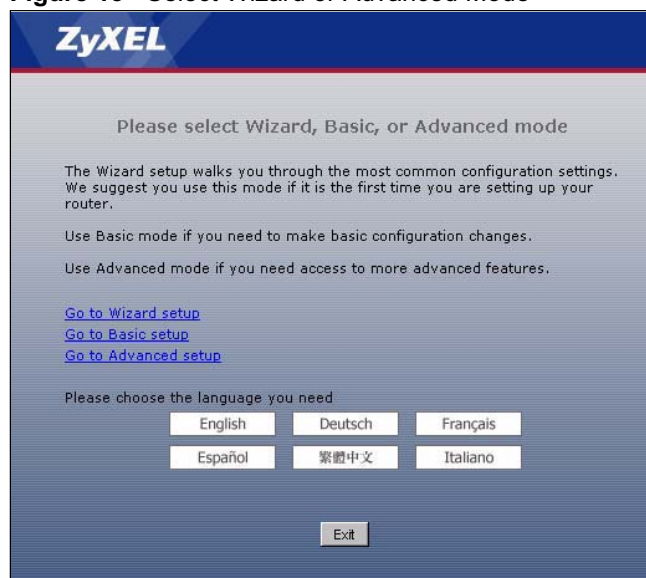
This chapter provides information on the wizard setup screens in the web configurator.

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 NBG420N 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 13 Select Wizard or Advanced Mode



- 2 Choose a language by clicking on the language's button. The screen will update. Click the **Next** button to proceed to the next screen.

Figure 14 Select a Language



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

Figure 15 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 **NBG420N 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 NBG420N via DHCP.

Click **Next** to configure the NBG420N for Internet access.

Figure 16 Wizard Step 1: System Information

The following table describes the labels in this screen.

Table 10 Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG420N 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 17 Wizard Step 2: Wireless LAN

STEP 1 > STEP 2 > STEP 3 > STEP 4

WIRELESS LAN

WIRELESS LAN

The SSID is the name given to your wireless network. It may be possible to see multiple wireless networks from your home or office, so choose a name that you will be able to recognize later.

Name (SSID)

Security

Channel Selection **Auto**

In addition to the connection wizard, you can also use Windows Vista WPS to change the WLAN settings.

<Back Next > Exit

The following table describes the labels in this screen.

Table 11 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 NBG420N, 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 (WPA2-PSK) to have the NBG420N generate a pre-shared key automatically. After you click Next a screen pops up displaying the generated pre-shared key. 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 NBG420N, 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 54 . 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 53 . This option is only available if WPS is not enabled. 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 54 .
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. The device will automatically select the channel with the least interference.
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 NBG420N 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 18 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 12 Wizard Step 2: Basic (WEP) Security

LABEL	DESCRIPTION
Passphrase	Type a Passphrase (up to 32 printable characters) and click Generate . The NBG420N 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 NBG420N 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 12 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 19 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

The following table describes the labels in this screen.

Table 13 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 NBG420N 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 20 Wizard Step 3: ISP Parameters.

The following table describes the labels in this screen,

Table 14 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 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. Continue to [Section 4.4.4 on page 58](#).

Figure 21 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 NBG420N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG420N 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 22 Wizard Step 3: PPPoE Connection

The following table describes the labels in this screen.

Table 15 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 NBG420N supports one PPTP server connection at any given time.

Figure 23 Wizard Step 3: PPTP Connection

The following table describes the fields in this screen

Table 16 Wizard Step 3: PPTP Connection

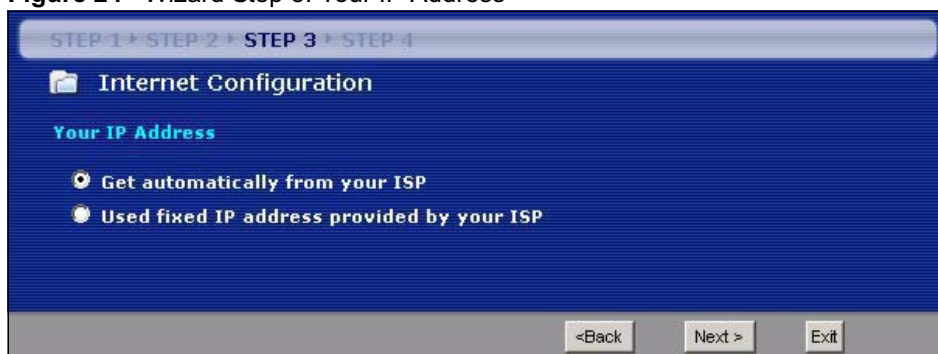
LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select PPTP from the drop-down list box. To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
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.
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 NBG420N 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).
Back	Click Back to return to the previous screen.

Table 16 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 NBG420N an automatically assigned IP address depending on your ISP.

Figure 24 Wizard Step 3: Your IP Address

The following table describes the labels in this screen

Table 17 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 on page 61 .
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 18 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 NBG420N, 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 NBG420N 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 NBG420N 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 NBG420N 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.

- 2 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 25 Wizard Step 3: WAN IP and DNS Server Addresses

The screenshot shows a wizard interface with a blue background. At the top, there are navigation tabs for STEP 1, STEP 2, STEP 3 (selected), and STEP 4. Below the tabs is a folder icon and the text 'Internet Configuration'. Underneath, there are two sections: 'WAN IP Address Assignment' and 'DNS Server Address Assignment'. Each section contains three text input fields. The WAN IP Address field contains '172.23.23.49', the Subnet Mask field contains '255.255.255.0', and the Gateway IP Address field contains '0.0.0.0'. The DNS Server section has three fields: 'First DNS Server' with '172.23.5.1', 'Second DNS Server' with '172.23.5.2', and 'Third DNS Server' with '0.0.0.0'. At the bottom of the screen, there are three buttons: '<Back', 'Next >', and 'Exit'.

The following table describes the labels in this screen

Table 19 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 NBG420N 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

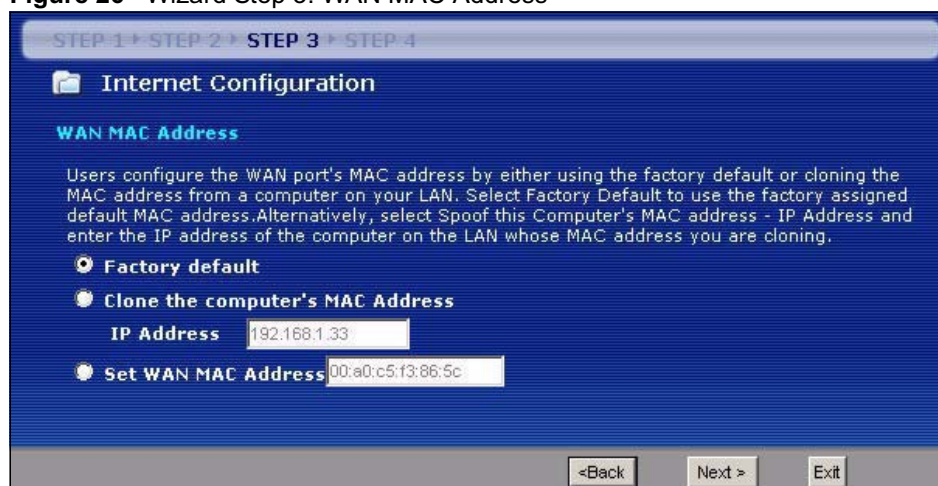
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Table 20 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(NBG420N LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the NBG420N'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 26 Wizard Step 3: WAN MAC Address



The following table describes the fields in this screen.

Table 21 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 NBG420N'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 27 Wizard Step 4: Bandwidth Management



The following fields describe the label in this screen.

Table 22 Wizard Step 4: Bandwidth Management

LABEL	DESCRIPTION
Enable BM for all traffic automatically	Select the check box to have the NBG420N apply bandwidth management to traffic going out through the NBG420N'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 28 Connection Wizard Save

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

Figure 29 Connection Wizard Complete

Well done! You have successfully set up your NBG420N to operate on your network and access the Internet.

AP Mode

This chapter discusses how to configure settings while your NBG420N is set to **AP Mode**. Many screens that are available in **Router Mode** are not available in **AP Mode**.

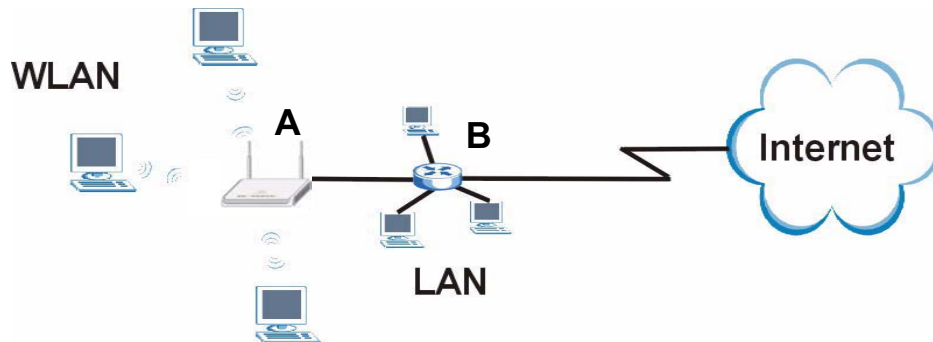


See [Chapter 6 on page 73](#) for an example of setting up a wireless network in AP mode.

5.1 AP Mode Overview

Use your NBG420N as an AP if you already have a router or gateway on your network. In this mode your device bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

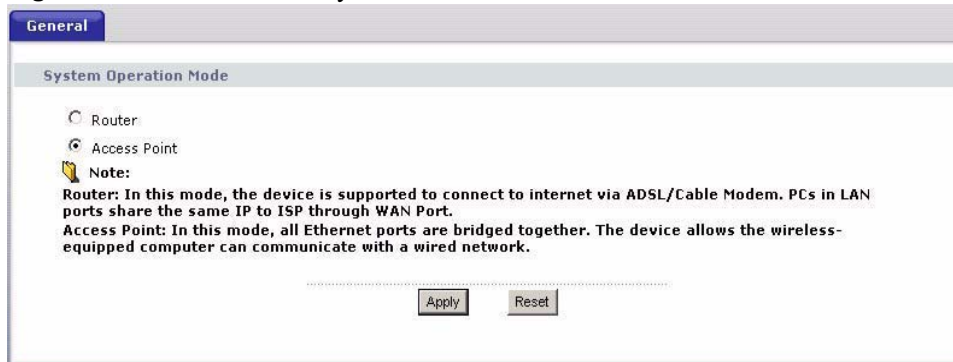
Figure 30 Wireless Internet Access in AP Mode



5.2 Setting your NBG420N to AP Mode

- 1 Log into the web configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To set your NBG420N to **AP Mode**, go to **Maintenance > Sys OP Mode > General** and select **Access Point**.

Figure 31 Maintenance > Sys OP Mode > General



- 3 A pop-up appears providing information on this mode. Click **OK** in the pop-up message window. (See [Section 24.2 on page 260](#) for more information on the pop-up.) Click **Apply**. Your NBG420N is now in AP Mode.

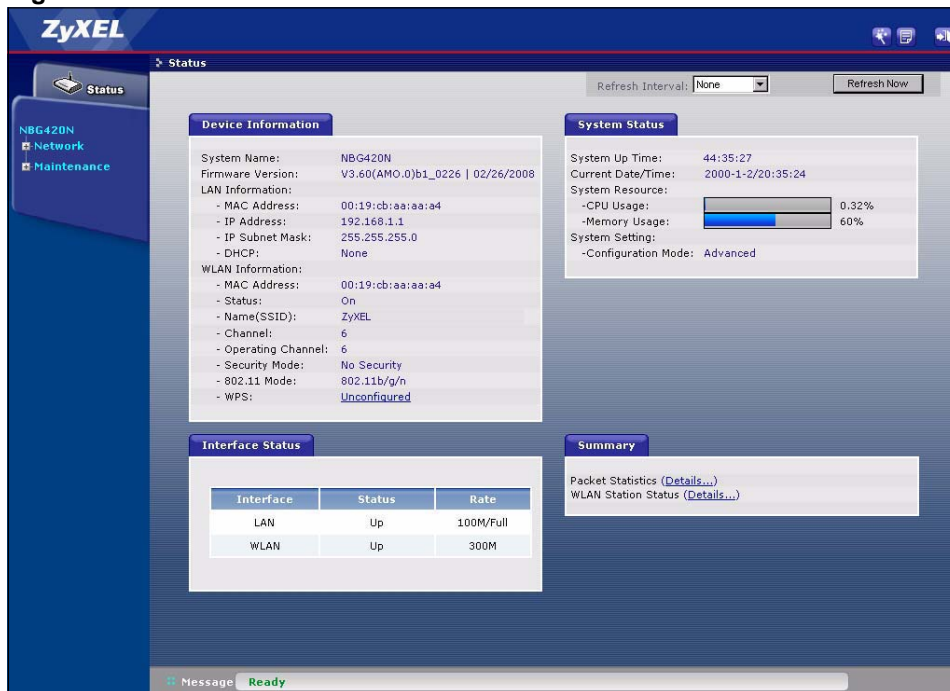


You do not have to log in again or restart your device when you change modes.

5.3 The Status Screen in AP Mode

Click on **Status**. The screen below shows the status screen in **AP Mode**.

Figure 32 Status: AP Mode



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

Table 23 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 firmware version and the date created.
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 - Client or None .
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - On , Off or Off by scheduler .
- Name (SSID)	This shows a descriptive name used to identify the NBG420N in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG420N is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG420N is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the NBG420N supports. Wireless clients must support the same standard in order to be able to connect to the NBG420N
- WPS	This shows the WPS (WiFi Protected Setup) Status. Click the status to display Network > Wireless LAN > WPS screen.
System Status	
System Uptime	This is the total time the NBG420N has been on.
Current Date/Time	This field displays your NBG420N's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG420N's processing ability is currently used. When this percentage is close to 100%, the NBG420N 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 NBG420N 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	
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (Advanced) or not (Basic).
Interface Status	
Interface	This displays the NBG420N port types. The port types are: LAN and WLAN .
Status	For the LAN port, 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.

Table 23 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
Rate	For the LAN ports, this displays the port speed and duplex setting or 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.
Summary	
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 NBG420N.

5.3.1 Navigation Panel

Use the menu in the navigation panel to configure NBG420N features in **AP Mode**.

The following screen and table show the features you can configure in **AP Mode**.

Figure 33 Menu: AP Mode

The following table describes the sub-menus.

Table 24 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG420N's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		

Table 24 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 NBG420N to block access to devices or block the devices from accessing the NBG420N.
	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.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	IP	Use this screen to configure LAN IP address and subnet mask or to get the LAN IP address from a DHCP server.
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 NBG420N'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 NBG420N's log settings.
Tools	Firmware	Use this screen to upload firmware to your NBG420N.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG420N.
	Restart	This screen allows you to reboot the NBG420N without turning the power off.
	Wake On LAN	Use this screen to remotely turn on a device on the network.
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 whether your device acts as a Router or a Access Point.
Language		This screen allows you to select the language you prefer.

5.4 Configuring Your Settings

5.4.1 LAN Settings

Use this section to configure your LAN settings while in **AP Mode**.

Click **Network > LAN** to see the screen below.



If you change the IP address of the NBG420N in the screen below, you will need to log into the NBG420N again using the new IP address.

Figure 34 Network > LAN > IP

The screenshot shows the 'IP' configuration page for the NBG420N. It is divided into two main sections: 'LAN TCP/IP' and 'DNS Servers'. In the 'LAN TCP/IP' section, the 'User Defined LAN IP' radio button is selected. Below it, there are three input fields: 'IP Address' (192.168.1.1), 'IP Subnet Mask' (255.255.255.0), and 'Gateway IP Address' (0.0.0.0). The 'DNS Servers' section has three rows, each with a dropdown menu set to 'From ISP' and a corresponding IP address field: 'First DNS Server' (172.23.5.2), 'Second DNS Server' (172.23.5.1), and 'Third DNS Server' (0.0.0.0). At the bottom, there are 'Apply' and 'Reset' buttons.

The table below describes the labels in the screen.

Table 25 Network > LAN > IP

LABEL	DESCRIPTION
Get from DHCP Server	Select this option to allow the NBG420N to obtain an IP address from a DHCP server on the network. You must connect the WAN port to a device with a DHCP server enabled (such as a router or gateway). Without a DHCP server the NBG420N will have no IP address. You need to find out the IP address the DHCP server assigns to the NBG420N and use that address to log in to the NBG420N again.
User Defined LAN IP	Select this option to set the NBG420N's IP address. This setting is selected by default. Check the IP address is on the same domain as other devices on your network.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.1. If you change the IP address you will have to log in again with the new IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG420N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG420N.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your NBG420N that will forward the packet to the destination. In AP Mode , the gateway must be a router on the same segment as your NBG420N.
DNS Servers	
First DNS Server	Select From ISP if your ISP dynamically assigns DNS server information. The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
Second DNS Server	Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply .
Third DNS Server	Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the NBG420N.
Reset	Click Reset to reload the previous configuration for this screen.

5.4.2 WLAN and Maintenance Settings

The configuration of wireless and maintenance settings in **AP Mode** is the same as for **Router Mode**.

- See [Chapter 5 on page 69](#) for information on the configuring your wireless network.
- See [Maintenance and Troubleshooting \(227\)](#) for information on the configuring your Maintenance settings.

5.5 Logging in to the Web Configurator in AP Mode

- 1 Connect your computer to the LAN port of the NBG420N.
- 2 The default IP address of the NBG420N is “192.168.1.1”. In this case, your computer must have an IP address in the range between “192.168.1.2” and “192.168.1.255”.
- 3 Click **Start > Run** on your computer in Windows.
- 4 Type “cmd” in the dialog box.
- 5 Type “ipconfig” to show your computer’s IP address. If your computer’s IP address is not in the correct range then see [Appendix D on page 293](#) for information on changing your computer’s IP address.
- 6 After you’ve set your computer’s IP address, open a web browser such as Internet Explorer and type “192.168.1.1” as the web address in your web browser.

See [Chapter 6 on page 73](#) for a tutorial on setting up a network with an AP.

Tutorials

6.1 Wireless Tutorials

6.1.1 How to Connect to the Internet from an AP

This section gives you an example of how to set up an access point (AP) and wireless client (a notebook (B), in this example) for wireless communication. B can access the Internet through the AP wirelessly.

Figure 35 Wireless AP Connection to the Internet



6.1.2 Configure Wireless Security Using WPS on both your NBG420N and Wireless Client

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG420N as the AP and NWD210N as the wireless client which connects to a notebook.



The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section 6.1.2.1 on page 74](#). This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG420N's interface. See [Section 6.1.2.2 on page 75](#). This is the more secure method, since one device can authenticate the other.

6.1.2.1 Push Button Configuration (PBC)

- 1 Make sure that your NBG420N is turned on and that it is within range of your computer.
- 2 Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
- 3 In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
- 4 Log into NBG420N's web configurator and press the **Push Button** button in the **Network > Wireless Client > WPS Station** screen.



Your NBG420N has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

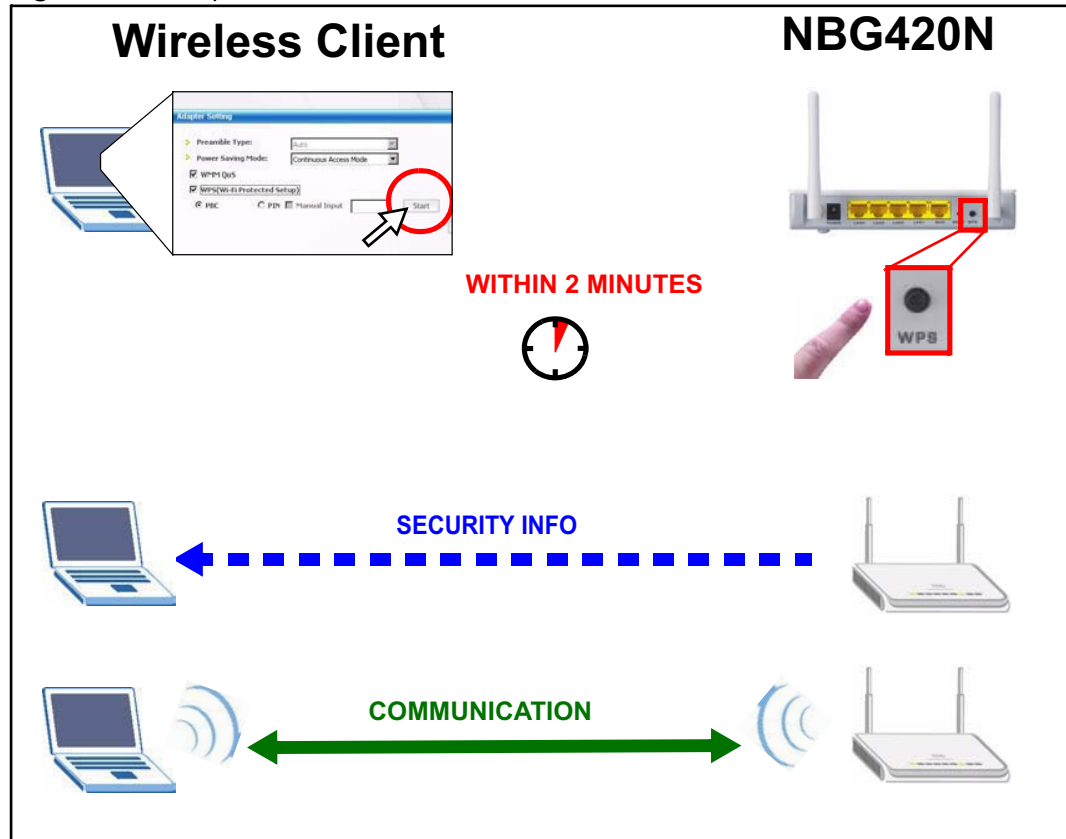


It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The NBG420N sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG420N securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG420N and wireless client (the NWD210N in this example).

Figure 36 Example WPS Process: PBC Method



6.1.2.2 PIN Configuration

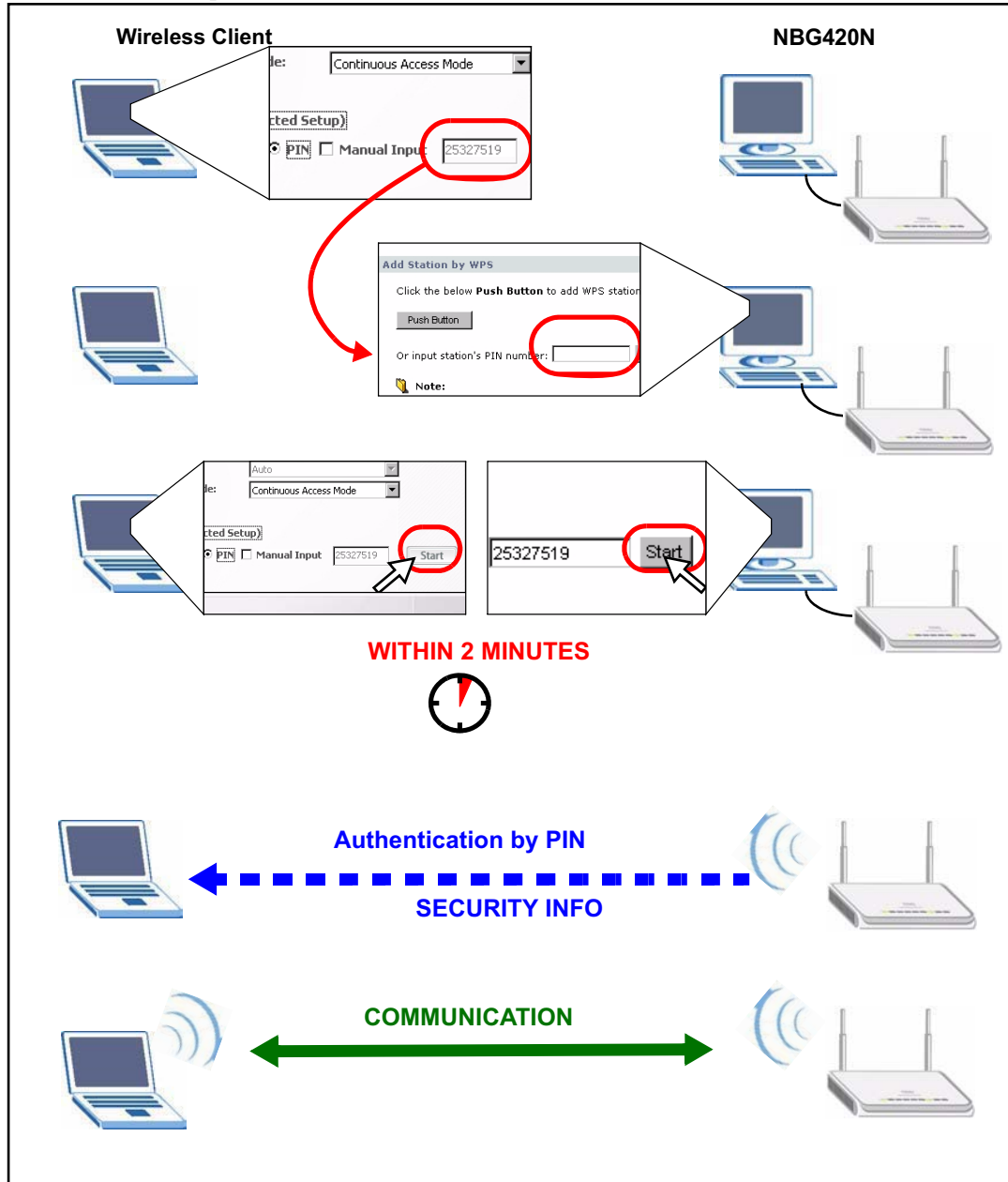
When you use the PIN configuration method, you need to use both NBG420N's configuration interface and the client's utilities.

- 1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
- 2 Enter the PIN number to the **PIN** field in the **Network > Wireless LAN > WPS Station** screen on the NBG420N.
- 3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG420N's **WPS Station** screen within two minutes.

The NBG420N authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG420N securely.

The following figure shows you the example to set up wireless network and security on NBG420N and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 37 Example WPS Process: PIN Method



6.1.3 Enable and Configure Wireless Security without WPS on your NBG420N

This example shows you how to configure wireless security settings with the following parameters on your NBG420N.

SSID	SSID_Example3
------	---------------

Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG420N.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the web configurator through your LAN connection (see [Section 3.2 on page 37](#)).

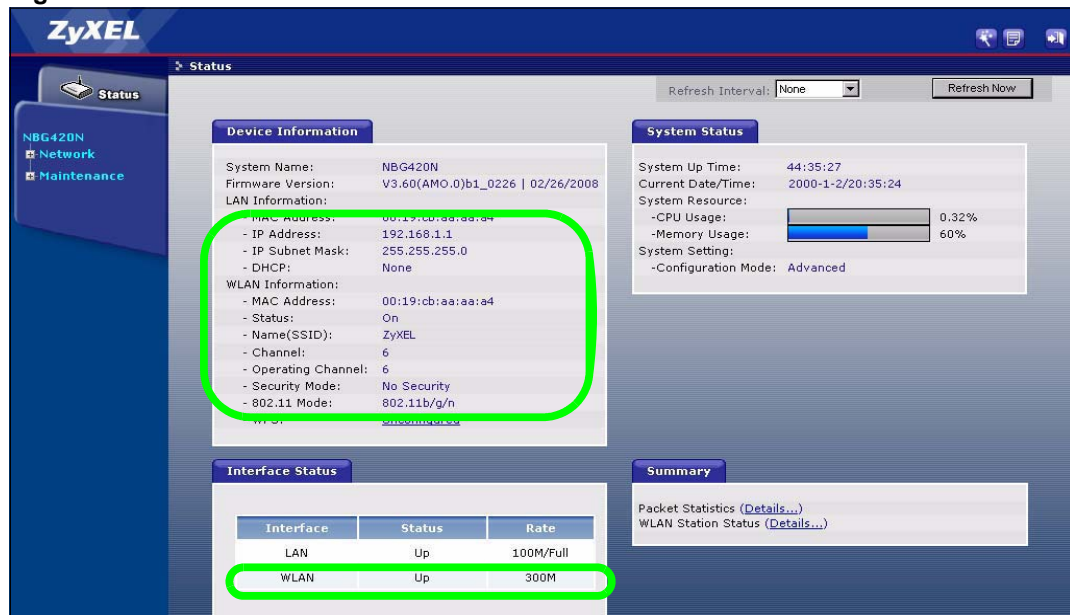
- 1 Open the **Wireless LAN > General** screen in the AP's web configurator.
- 2 Make sure the **Enable Wireless LAN** check box is selected.
- 3 Enter **SSID_Example3** as the SSID and select a channel.
- 4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 38 Network > Wireless LAN > General

The screenshot shows the configuration page for Wireless LAN > General. The 'Enable Wireless LAN' checkbox is checked. The SSID is set to 'SSID_Example3'. The channel is set to 'Channel-06 2437MHz'. The security mode is set to 'WPA-PSK' and the pre-shared key is 'ThisismyWPA-PSKpre-sharedkey'. The 'Apply' button is highlighted.

- 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 39 Status: AP Mode

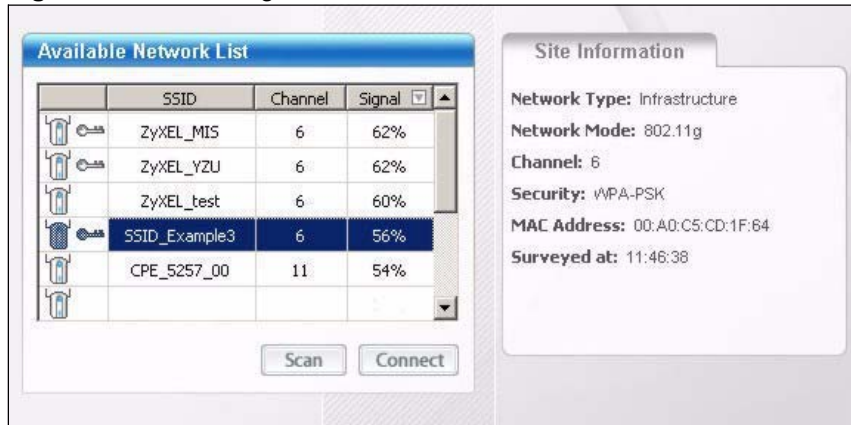


6.1.4 Configure Your Notebook

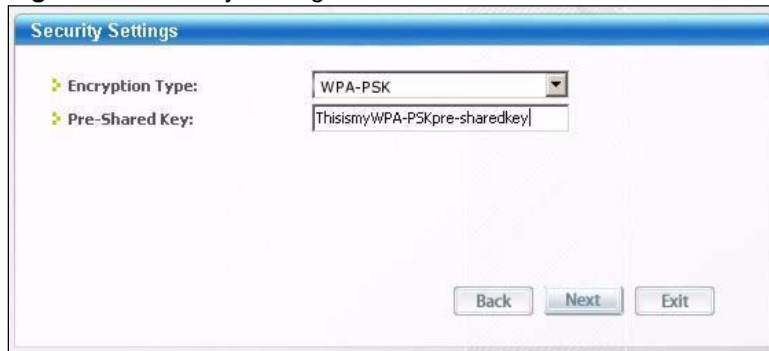


We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

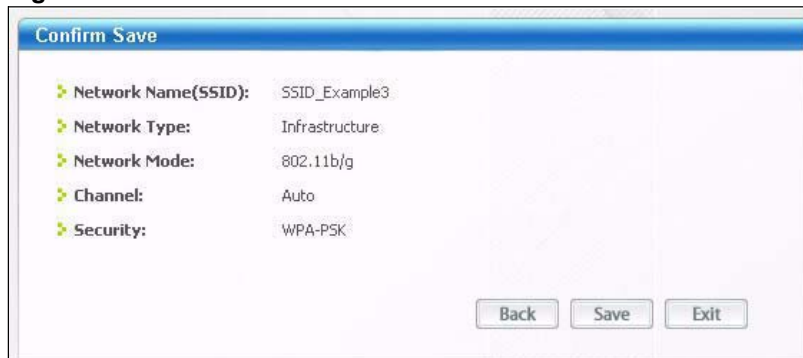
- 1 The NBG420N supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.
- 2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.
- 3 After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.
- 4 Select SSID_Example3 and click **Connect**.

Figure 40 Connecting a Wireless Client to a Wireless Network

5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 41 Security Settings

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

Figure 42 Confirm Save

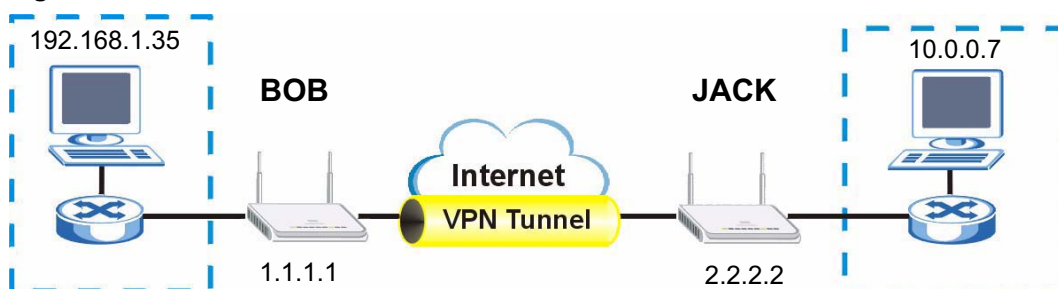
7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 43 Link Status

- 8 If your connection is successful, 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.

6.2 Site-To-Site VPN Tunnel Tutorial

Bob and Jack want to setup a VPN connection between their offices. Bob and Jack each have a NBG420N router and a static WAN IP address. This tutorial covers how to configure their NBG420Ns to create a secure connection.

Figure 44 Site-To-Site VPN Tunnel

The following table describes the VPN settings that must be configured on Bob and Jack's NBG420N routers.

Table 26 Site-To-Site VPN Tunnel Settings

SETTING	BOB	JACK
Active	YES	YES
IPSec Keying Mode	IKE	IKE
Local Address	192.168.1.35	10.0.0.7
Local Address End /Mask	192.168.1.35	10.0.0.7
Remote Address	10.0.0.7	192.168.1.35
Remote Address End /Mask	10.0.0.7	192.168.1.35
My IP Address	1.1.1.1	2.2.2.2

Table 26 Site-To-Site VPN Tunnel Settings (continued)

SETTING	BOB	JACK
Local ID Type	IP	IP
Local Content	1.1.1.1	2.2.2.2
Secure Gateway Address	2.2.2.2	1.1.1.1
Peer ID Type	IP	IP
Peer Content	2.2.2.2	1.1.1.1
Encapsulation Mode	Tunnel	Tunnel
IPSec Protocol	ESP	ESP
Pre-Shared Key	ThisIsMySecretKey	ThisIsMySecretKey
Encryption Algorithm	3DES	3DES
Authentication Algorithm	SHA1	SHA1

6.2.1 Configuring Bob's NBG420N VPN Settings

To configure these settings Bob uses the NBG420N web configurator.

- 1 Log into the NBG420N web configurator and click **VPN > Modify** icon. This displays the VPN Rule Setup (Basic) screen.
- 2 Select the **Active** checkbox to make the VPN rule active after it has been created. Make sure IKE is selected as the **IPSec Keying Mode**.

Figure 45 Property

- 3 Enter the IP address “192.168.1.35” into the **Local Address** text box. This is the IP address of Bob’s computer. Enter the IP address “192.168.1.35” into the **Local Address End/Mask** text box. This value is the same as Bob only wants Jack to access this single IP address.

Figure 46 Local Policy

- 4 Enter the IP address “10.0.0.7” into the **Remote Address Start** text box. This is the IP address of Jack’s computer. Enter the IP address “10.0.0.7” into the **Remote Address**

End/Mask text box. This value is the same as Jack only wants Bob to access this single IP address.

Figure 47 Remote Policy

Remote Policy	
Remote Address Start	<input type="text" value="10.0.0.7"/>
Remote Address End/Mask	<input type="text" value="10.0.0.7"/>

- 5** Enter the IP address “1.1.1.1” into the **My IP Address** text box. This is Bob’s WAN IP address.
- 6** Select IP as the **Local ID Type**. This is the type of content that will be used to identify Bob’s NBG420N. Enter the IP address “1.1.1.1” into the **Local Content** text box. This identifies Bob’s NBG420N to Jack’s NBG420N.
- 7** Enter the IP address “2.2.2.2” into the **Secure Gateway Address** text box. This is Jack’s WAN IP address.
- 8** Select IP as the **Peer ID Type**. This is Jack’s **Local ID Type**. Enter “2.2.2.2” into the **Peer Content** text box. This is Jack’s **Local Content** WAN IP address.

Figure 48 Authentication Method

Authentication Method	
My IP Address	<input type="text" value="1.1.1.1"/>
Local ID Type	<input type="text" value="IP"/>
Local Content	<input type="text" value="1.1.1.1"/>
Secure Gateway Address	<input type="text" value="2.2.2.2"/>
Peer ID Type	<input type="text" value="IP"/>
Peer Content	<input type="text" value="2.2.2.2"/>





- 9** Select **Tunnel** as the **Encapsulation Mode** and **ESP** as the **IPSec Protocol**.
- 10** Enter “ThisIsMySecretKey” as the **Pre-Shared Key**. This is the password for the VPN tunnel that only Bob and Jack know.
- 11** Select **3DES** as the encryption algorithm. Select the authentication algorithm as **SHA1**. These algorithms are more secure.

Figure 49 IPSec Algorithm

IPSec Algorithm	
Encapsulation Mode	<input type="text" value="Tunnel"/>
IPSec Protocol	<input type="text" value="ESP"/>
Pre-Shared Key	<input type="text" value="ThisIsMySecretKey"/>
Encryption Algorithm	<input type="text" value="3DES"/>
Authentication Algorithm	<input type="text" value="SHA1"/>

- 12** Click **Apply** to save the new rule and click VPN to return to the VPN Summary screen. The new VPN rule is displayed as shown below.

Figure 50 VPN Summary

VPN Summary							
#	Active	Local Addr.	Remote Addr.	Encap.	Algorithm	Gateway	Modify
1	<input checked="" type="checkbox"/>	192.168.1.35	10.0.0.7	Tunnel	ESP-3DES-SHA1	2.2.2.2	 
2	<input type="checkbox"/>						 

6.2.2 Configuring Jack's NBG420N VPN Settings

To configure these settings Jack uses the NBG420N web configurator.

- 1 Log into the NBG420N web configurator and click **VPN > Modify** icon. This displays the VPN Rule Setup (Basic) screen.
- 2 Select the **Active** checkbox to make the VPN rule active after it has been created. Make sure IKE is selected as the **IPSec Keying Mode**.

Figure 51 Property

Property	
<input checked="" type="checkbox"/>	Active
<input type="checkbox"/>	Keep Alive
<input type="checkbox"/>	NAT Traversal
IPSec Keying Mode	IKE
DNS Server (for IPSec VPN)	0.0.0.0

- 3 Enter the IP address "10.0.0.7" into the **Local Address** text box. This is the IP address of Jack's computer. Enter the IP address "10.0.0.7" into the **Local Address End/Mask** text box. This value is the same as Jack only wants Bob to access this single IP address.

Figure 52 Local Policy

Local Policy	
Local Address	10.0.0.7
Local Address End/Mask	10.0.0.7

- 4 Enter the IP address "192.168.1.35" into the **Remote Address Start** text box. This is the IP address of Jack's computer. Enter the IP address "192.168.1.35" into the **Remote Address End/Mask** text box. This value is the same as Bob only wants Jack to access this single IP address.

Figure 53 Remote Policy

Remote Policy	
Remote Address Start	192.168.1.35
Remote Address End/Mask	192.168.1.35

- 5 Enter the IP address "2.2.2.2" into the **My IP Address** text box. This is Jack's WAN IP address.

- 6 Select IP as the **Local ID Type**. This is the type of content that will be used to identify Jack's NBG420N. Enter the IP address "2.2.2.2" into the **Local Content** text box. This identifies Jack's NBG420N to Bob's NBG420N.
- 7 Enter the IP address "1.1.1.1" into the **Secure Gateway Address** text box. This is Bob's WAN IP address.
- 8 Select IP as the **Peer ID Type**. This is Bob's **Local ID Type**. Enter "1.1.1.1" into the **Peer Content** text box. This is Bob's **Local Content** WAN IP address.

Figure 54 Authentication Method

Authentication Method	
My IP Address	2.2.2.2
Local ID Type	IP
Local Content	2.2.2.2
Secure Gateway Address	1.1.1.1
Peer ID Type	IP
Peer Content	1.1.1.1

- 9 Select **Tunnel** as the **Encapsulation Mode** and **ESP** as the **IPSec Protocol**.
- 10 Enter "ThisIsMySecretKey" as the **Pre-Shared Key**. This is the password for the VPN tunnel that only Bob and Jack know.
- 11 Select **3DES** as the encryption algorithm. Select the authentication algorithm as **SHA1**. These algorithms are more secure.

Figure 55 IPSec Algorithm

IPSec Algorithm	
Encapsulation Mode	Tunnel
IPSec Protocol	ESP
Pre-Shared Key	ThisIsMySecretKey
Encryption Algorithm	3DES
Authentication Algorithm	SHA1

- 12 Click **Apply** to save the new rule and click **VPN** in the web configurator menu to return to the VPN Summary screen. The new VPN rule is displayed as shown below.

Figure 56 VPN Summary

VPN Summary							
#	Active	Local Addr.	Remote Addr.	Encap.	Algorithm	Gateway	Modify
1		10.0.0.7	192.168.1.35	Tunnel	ESP-3DES-SHA1	1.1.1.1	
2							

6.2.3 Checking the VPN Connection

Check if the VPN connection is working by pinging the computer on the other side of the VPN connection. In the example below Bob is pinging Jack's computer.

Figure 57 Pinging Jack's Local IP Address

```

C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:>ping 10.0.0.7

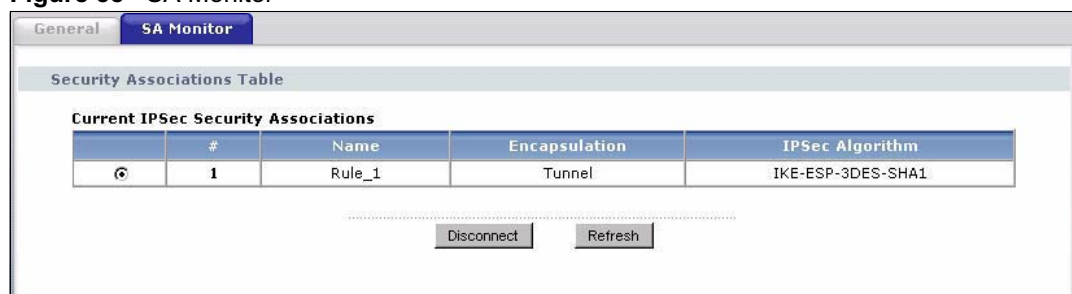
Pinging 10.0.0.7 with 32 bytes of data:

Reply from 10.0.0.7: bytes=32 time=2ms TTL=252
Reply from 10.0.0.7: bytes=32 time=2ms TTL=252
Reply from 10.0.0.7: bytes=32 time=2ms TTL=252
Reply from 10.0.0.7: bytes=32 time=2ms TTL=252

Ping statistics for 10.0.0.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

```

Pinging is successful which means a VPN tunnel has been established between Bob and Jack's NBG420Ns. Congratulations! To monitor this VPN connection click **VPN > SA Monitor** in the web configurator.

Figure 58 SA Monitor

If pinging is not successful check the VPN settings on both devices and try again. If you are still having problems make sure the VPN settings in the Advanced options are also the same.

For more information on VPN including field descriptions refer to [Chapter 15 on page 165](#).

PART II

Network

Wireless LAN (89)

WAN (117)

LAN (127)

DHCP (133)

Network Address Translation (NAT) (137)

Dynamic DNS (147)



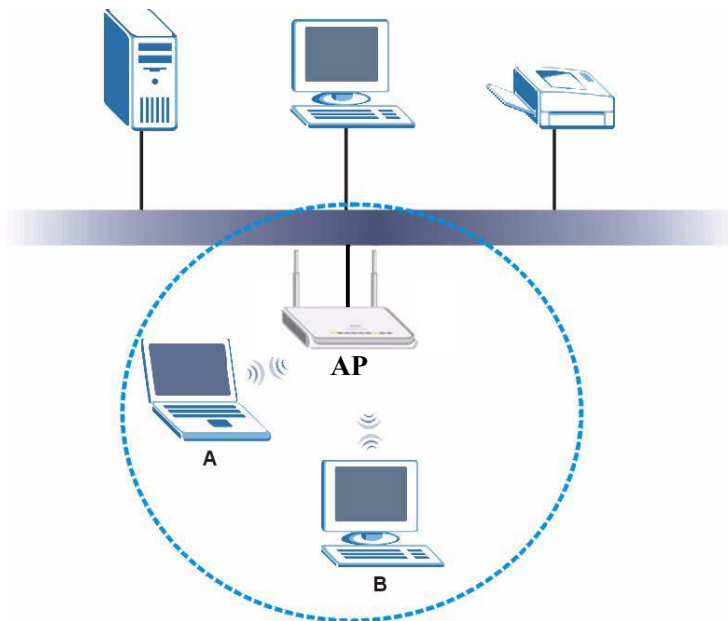
Wireless LAN

This chapter discusses how to configure the wireless network settings in your NBG420N. See the appendices for more detailed information about wireless networks.

7.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 59 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 NBG420N 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.

7.2 Wireless Security Overview

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

7.2.1 SSID

Normally, the 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.

7.2.2 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.

7.2.3 User Authentication

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

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

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

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

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

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


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

7.2.4 Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See [Section 7.2.3 on page 90](#) for information about this.)

Table 27 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 NBG420N, 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 NBG420N.

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.

7.3 Roaming

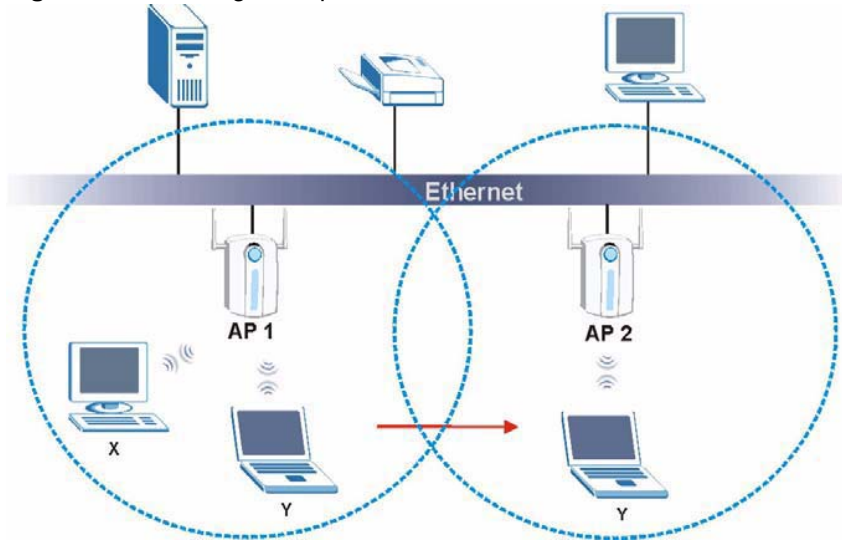
A wireless station is a device with an IEEE 802.11a/b/g/n compliant wireless interface. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the 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 60 on page 93](#).

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 60 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**.

7.3.1 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.

7.4 Quality of Service

This section discusses the Quality of Service (QoS) features available on the NBG420N.

7.4.1 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 NBG420N uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q tag or DSCP information in each packet's header. The NBG420N 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).

7.4.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the NBG420N uses.

Table 28 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.

7.5 General Wireless LAN Screen



If you are configuring the NBG420N from a computer connected to the wireless LAN and you change the NBG420N'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 NBG420N's new settings.

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

Figure 61 Network > Wireless LAN > General

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

Table 29 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 the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if Auto Channel Selection is disabled.
Auto Channel Selection	Select this check box for the NBG420N to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the Channel Section field.
Operating Channel	This displays the channel the NBG420N is currently using.
Channel Width	Select whether the NBG420N uses a wireless channel width of 20 or 40 MHz. A standard 20 MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. Because not all devices support 40 MHz channels, select Auto 20/40MHz to allow the NBG420N to adjust the channel bandwidth automatically.
Security Mode	Select Static-WEP , WPA-PSK , WPA , WPA2-PSK , or WPA2 to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See 7.5.2, 7.5.3, 7.5.4 sections. Or you can select No Security to allow any client to associate this network without authentication. Note: If you enable the WPS function, only No Security , WPA-PSK and WPA2-PSK are available in this field.

Table 29 Network > Wireless LAN > General

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the NBG420N.
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.

7.5.1 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 NBG420N, your network is accessible to any wireless networking device that is within range.

Figure 62 Network > Wireless LAN > General: No Security

The screenshot shows the configuration page for 'Wireless LAN > General: No Security'. The 'Wireless Setup' section includes:

- Enable Wireless LAN
- Name(SSID): ZyXEL
- Hide SSID
- Channel Selection: Channel-01 2412MHz
- Operating Channel: Channel-006
- Channel Width: Auto 20/40 MHz
- Auto Channel Selection

 The 'Security' section shows:

- Security Mode: No Security
- Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled

The following table describes the labels in this screen.

Table 30 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose No Security from the drop-down list box.
Apply	Click Apply to save your changes back to the NBG420N.
Reset	Click Reset to reload the previous configuration for this screen.

7.5.2 WEP Encryption

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

Your NBG420N allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

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

Figure 63 Network > Wireless LAN > General: Static WEP

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

Table 31 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Passphrase	Enter a passphrase (password phrase) of up to 32 printable characters and click Generate . The NBG420N automatically generates four different WEP keys and displays them in the Key fields below.
WEP Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	This field is activated when you select 64-bit WEP or 128-bit WEP in the WEP Encryption field. Select Auto or Shared Key from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.

Table 31 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NBG420N 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.
Apply	Click Apply to save your changes back to the NBG420N.
Reset	Click Reset to reload the previous configuration for this screen.

7.5.3 WPA-PSK/WPA2-PSK

Click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 64 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

The screenshot shows the configuration page for WPA-PSK/WPA2-PSK security mode. The page is divided into two main sections: **Wireless Setup** and **Security**.

Wireless Setup:

- Enable Wireless LAN
- Name(SSID): ZyXEL
- Hide SSID
- Channel Selection: Channel-06 2437MHz (dropdown menu)
- Auto Channel Selection:
- Operating Channel: Channel-006
- Channel Width: Auto 20/40 MHz (dropdown menu)

Security:

- Security Mode: WPA2-PSK (dropdown menu)
- WPA Compatible
- Pre-Shared Key: [Empty text field]
- ReAuthentication Timer: 0 (In Seconds, 0 means no ReAuthentication)
- Idle Timeout: 3600 (In Seconds)
- Group Key Update Timer: 1800 (In Seconds)

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

The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG420N even when the NBG420N is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The NBG420N automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA/WPA2 key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. The default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes back to the NBG420N.
Reset	Click Reset to reload the previous configuration for this screen.

7.5.4 WPA/WPA2

Click **Network > Wireless LAN** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 65 Network > Wireless LAN > General: WPA/WPA2

The following table describes the labels in this screen.

Table 33 Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG420N even when the NBG420N is using WPA2-PSK or WPA2.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The NBG420N automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).