

# NBG-419N

Wireless N Home Router

**DRAFT**

## User's Guide

### Default Login Details

IP Address	http://192.168.1.1
Password	1234

Firmware Version 1.0  
Edition 2, 5/2009

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



# ZyXEL

Copyright © 2009  
ZyXEL Communications Corporation

Company Confidential

# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the NBG-419N 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.

- Supporting Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

Please refer to [www.zyxel.com](http://www.zyxel.com) for additional support documentation and product certifications.

## User Guide Feedback

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

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

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

## Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See [http://www.zyxel.com/web/contact\\_us.php](http://www.zyxel.com/web/contact_us.php) for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.

Brief description of the problem and the steps you took to solve it.

# 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.**










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

## Syntax Conventions

- The NBG-419N may be referred to as the "NBG-419N", 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 NBG-419N icon is not an exact representation of your device.

NBG-419N 	Computer 	Notebook computer 
Server 	Modem 	Firewall 
Telephone 	Switch 	Router 

# Safety Warnings

- 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.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Company Confidential



# Contents Overview

<b>Introduction .....</b>	<b>19</b>
Getting to Know Your NBG-419N .....	21
Connection Wizard .....	25
Introducing the Web Configurator .....	37
Monitor .....	43
NBG-419N Modes .....	49
Easy Mode .....	51
Router Mode .....	63
Access Point Mode .....	71
WISP Mode .....	79
Tutorials .....	89
<b>Network .....</b>	<b>97</b>
Wireless LAN .....	99
WAN .....	119
LAN .....	135
DHCP Server .....	139
Network Address Translation (NAT) .....	143
Dynamic DNS .....	151
Static Route .....	153
RIP .....	157
<b>Security .....</b>	<b>159</b>
Firewall .....	161
Content Filter .....	167
<b>Management .....</b>	<b>171</b>
Bandwidth Management .....	173
Remote Management .....	183
Universal Plug-and-Play (UPnP) .....	187
<b>Maintenance and Troubleshooting .....</b>	<b>195</b>
Maintenance .....	197
Password .....	199
Time .....	201
Firmware Upgrade .....	205
Backup/Restore .....	207

Reset/Restart .....	211
Sys OP Mode .....	213
Troubleshooting .....	217
<b>Appendices and Index .....</b>	<b>231</b>

Company Confidential

# Table of Contents

<b>About This User's Guide</b> .....	<b>3</b>
<b>Document Conventions</b> .....	<b>5</b>
<b>Safety Warnings</b> .....	<b>7</b>
<b>Contents Overview</b> .....	<b>9</b>
<b>Table of Contents</b> .....	<b>11</b>
<b>Part I: Introduction</b> .....	<b>19</b>
<b>Chapter 1</b>	
<b>Getting to Know Your NBG-419N</b> .....	<b>21</b>
1.1 Overview .....	21
1.2 Applications .....	21
1.3 Ways to Manage the NBG-419N .....	22
1.4 Good Habits for Managing the NBG-419N .....	22
1.5 LEDs .....	22
<b>Chapter 2</b>	
<b>Connection Wizard</b> .....	<b>25</b>
2.1 Overview .....	25
2.2 Accessing the Wizard .....	25
2.3 Connect to Internet .....	26
2.3.1 Connection Type: DHCP .....	27
2.3.2 Connection Type: Static IP .....	28
2.3.3 Connection Type: PPPoE .....	28
2.3.4 Connection Type: PPTP .....	30
2.3.5 Connection Type: L2TP .....	31
2.4 Router Password .....	33
2.5 Wireless Security .....	33
2.5.1 Wireless Security: No Security .....	33
2.5.2 Wireless Security: WPA-PSK/WPA2-PSK .....	34
<b>Chapter 3</b>	
<b>Introducing the Web Configurator</b> .....	<b>37</b>
3.1 Overview .....	37

3.2 Accessing the Web Configurator .....	37
3.2.1 Login Screen .....	38
3.2.2 Password Screen .....	39
3.2.3 Home Screen .....	39
3.3 Resetting the NBG-419N .....	41
3.3.1 Procedure to Use the Reset Button .....	42
<b>Chapter 4</b>	
<b>Monitor.....</b>	<b>43</b>
4.1 Overview .....	43
4.2 What You Can Do .....	43
4.3 BW MGMT Monitor .....	43
4.4 DHCP Table .....	44
4.5 Packet Statistics .....	45
4.6 WLAN Station Status .....	46
<b>Chapter 5</b>	
<b>NBG-419N Modes.....</b>	<b>49</b>
5.1 Overview .....	49
5.1.1 Web Configurator Modes .....	49
5.1.2 Device Modes .....	49
<b>Chapter 6</b>	
<b>Easy Mode.....</b>	<b>51</b>
6.1 Overview .....	51
6.2 What You Can Do .....	52
6.3 What You Need to Know .....	52
6.4 Navigation Panel .....	53
6.5 Network Map .....	53
6.6 Control Panel .....	54
6.6.1 Game Engine .....	55
6.6.2 Power Saving .....	56
6.6.3 Content Filter .....	57
6.6.4 Bandwidth MGMT .....	58
6.6.5 Firewall .....	58
6.6.6 Wireless Security .....	59
6.6.7 WPS .....	60
6.7 Status Screen in Easy Mode .....	61
<b>Chapter 7</b>	
<b>Router Mode.....</b>	<b>63</b>
7.1 Overview .....	63
7.2 What You Can Do .....	63

7.3 Status Screen .....	64
7.3.1 Navigation Panel .....	67
<b>Chapter 8</b>	
<b>Access Point Mode .....</b>	<b>71</b>
8.1 Overview .....	71
8.2 What You Can Do .....	71
8.3 What You Need to Know .....	72
8.3.1 Setting your NBG-419N to AP Mode .....	72
8.3.2 Accessing the Web Configurator in Access Point Mode .....	73
8.3.3 Configuring your WLAN, Bandwidth Management and Maintenance Settings .....	73
8.4 AP Mode Status Screen .....	74
8.5 LAN Screen .....	76
<b>Chapter 9</b>	
<b>WISP Mode .....</b>	<b>79</b>
9.1 Overview .....	79
9.2 What You Can Do .....	79
9.3 What You Need to Know .....	80
9.3.1 Setting your NBG-419N to WISP Mode .....	80
9.3.2 Accessing the Web Configurator in WISP Mode .....	80
9.4 WISP Mode Status Screen .....	81
9.5 Wireless LAN General Screen .....	84
9.5.1 Static WEP .....	85
9.5.2 WPA(2)-PSK .....	87
9.5.3 Advance Screen .....	88
<b>Chapter 10</b>	
<b>Tutorials .....</b>	<b>89</b>
10.1 Overview .....	89
10.2 Connecting to the Internet from an Access Point .....	89
10.3 Configuring Wireless Security Using WPS .....	89
10.3.1 Push Button Configuration (PBC) .....	90
10.3.2 PIN Configuration .....	91
10.4 Enabling and Configuring Wireless Security (No WPS) .....	93
10.4.1 Configure Your Notebook .....	94
<b>Part II: Network .....</b>	<b>97</b>
<b>Chapter 11</b>	
<b>Wireless LAN .....</b>	<b>99</b>

11.1 Overview .....	99
11.2 What You Can Do .....	100
11.3 What You Should Know .....	100
11.3.1 Wireless Security Overview .....	100
11.4 General Wireless LAN Screen .....	103
11.4.1 No Security .....	104
11.4.2 WEP Encryption .....	105
11.4.3 WPA-PSK/WPA2-PSK .....	108
11.5 MAC Filter .....	109
11.6 Wireless LAN Advanced Screen .....	110
11.7 Quality of Service (QoS) Screen .....	111
11.8 WPS Screen .....	112
11.9 WPS Station Screen .....	113
11.10 Scheduling Screen .....	114
11.11 WDS Screen .....	115
<b>Chapter 12</b>	
<b>WAN .....</b>	<b>119</b>
12.1 Overview .....	119
12.2 What You Can Do .....	119
12.3 What You Need To Know .....	120
12.3.1 Configuring Your Internet Connection .....	120
12.3.2 Multicast .....	121
12.4 Internet Connection .....	122
12.4.1 Ethernet Encapsulation .....	122
12.4.2 PPPoE Encapsulation .....	124
12.4.3 PPTP Encapsulation .....	126
12.4.4 L2TP Encapsulation .....	129
12.5 Advanced WAN Screen .....	132
12.6 IGMP Snooping Screen .....	132
<b>Chapter 13</b>	
<b>LAN .....</b>	<b>135</b>
13.1 Overview .....	135
13.2 What You Can Do .....	135
13.3 What You Need To Know .....	136
13.3.1 IP Pool Setup .....	136
13.3.2 LAN TCP/IP .....	136
13.3.3 IP Alias .....	137
13.4 LAN IP Screen .....	137
13.5 IP Alias Screen .....	138
<b>Chapter 14</b>	
<b>DHCP Server .....</b>	<b>139</b>

14.1 Overview .....	139
14.2 What You Can Do .....	139
14.3 General Screen .....	139
14.4 Advanced Screen .....	140
<b>Chapter 15</b>	
<b>Network Address Translation (NAT) .....</b>	<b>143</b>
15.1 Overview .....	143
15.2 What You Can Do .....	144
15.3 General NAT Screen .....	144
15.4 NAT Application Screen .....	145
15.5 NAT Advanced Screen .....	147
15.5.1 Trigger Port Forwarding Example .....	149
15.5.2 Two Points To Remember About Trigger Ports .....	149
<b>Chapter 16</b>	
<b>Dynamic DNS .....</b>	<b>151</b>
16.1 Overview .....	151
16.2 What You Can Do .....	151
16.3 What You Need To Know .....	151
16.4 Dynamic DNS Screen .....	152
<b>Chapter 17</b>	
<b>Static Route .....</b>	<b>153</b>
17.1 Overview .....	153
17.2 What You Can Do .....	153
17.3 IP Static Route Screen .....	154
<b>Chapter 18</b>	
<b>RIP .....</b>	<b>157</b>
18.1 Overview .....	157
18.2 What You Can Do .....	157
18.3 RIP Screen .....	157
<b>Part III: Security .....</b>	<b>159</b>
<b>Chapter 19</b>	
<b>Firewall .....</b>	<b>161</b>
19.1 Overview .....	161
19.2 What You Can Do .....	162
19.3 What You Need To Know .....	162

19.4 General Firewall Screen .....	163
19.5 Services Screen .....	163
<b>Chapter 20</b>	
<b>Content Filter.....</b>	<b>167</b>
20.1 Overview .....	167
20.2 What You Can Do .....	167
20.3 What You Need To Know .....	167
20.3.1 Content Filtering Profiles .....	167
20.4 Content Filter Screen .....	168
<b>Part IV: Management .....</b>	<b>171</b>
<b>Chapter 21</b>	
<b>Bandwidth Management.....</b>	<b>173</b>
21.1 Overview .....	173
21.2 What You Can Do .....	173
21.3 What You Need To Know .....	174
21.4 General Screen .....	174
21.5 Advanced Screen .....	175
21.5.1 Rule Configuration: Application Rule Configuration .....	178
21.5.2 Rule Configuration: User Defined Service Rule Configuration .....	179
21.6 Monitor Screen .....	180
21.6.1 Predefined Bandwidth Management Services .....	181
<b>Chapter 22</b>	
<b>Remote Management.....</b>	<b>183</b>
22.1 Overview .....	183
22.2 What You Can Do .....	183
22.3 What You Need to Know .....	183
22.3.1 Remote Management and NAT .....	184
22.3.2 System Timeout .....	184
22.4 WWW Screen .....	184
<b>Chapter 23</b>	
<b>Universal Plug-and-Play (UPnP).....</b>	<b>187</b>
23.1 Overview .....	187
23.2 What You Can Do .....	187
23.3 What You Need to Know .....	187
23.3.1 NAT Traversal .....	187
23.3.2 Cautions with UPnP .....	188



---

23.4 UPnP Screen .....	188
23.5 Technical Reference .....	189
23.5.1 Using UPnP in Windows XP Example .....	189
23.5.2 Web Configurator Easy Access .....	191
<b>Part V: Maintenance and Troubleshooting .....</b>	<b>195</b>
<b>Chapter 24</b>	
<b>Maintenance .....</b>	<b>197</b>
24.1 Overview .....	197
24.2 What You Can Do .....	197
24.3 General Screen .....	197
<b>Chapter 25</b>	
<b>Password .....</b>	<b>199</b>
25.1 Overview .....	199
25.2 What You Can Do .....	199
25.3 What You Need to Know .....	199
25.4 Password Screen .....	200
<b>Chapter 26</b>	
<b>Time .....</b>	<b>201</b>
26.1 Overview .....	201
26.2 What You Can Do .....	201
26.3 Time Setting Screen .....	201
<b>Chapter 27</b>	
<b>Firmware Upgrade .....</b>	<b>205</b>
27.1 Overview .....	205
27.2 What You Can Do .....	205
27.3 Firmware Upload Screen .....	205
<b>Chapter 28</b>	
<b>Backup/Restore .....</b>	<b>207</b>
28.1 Overview .....	207
28.2 What You Can Do .....	207
28.3 Configuration Screen .....	208
<b>Chapter 29</b>	
<b>Reset/Restart .....</b>	<b>211</b>
29.1 Overview .....	211

29.2 What You Can Do .....	211
29.3 Reset/Restart Screen .....	211
<b>Chapter 30</b>	
<b>Sys OP Mode.....</b>	<b>213</b>
30.1 Overview .....	213
30.2 What You Can Do .....	213
30.3 What You Need to Know .....	213
30.4 Sys Op Mode Screen .....	215
<b>Chapter 31</b>	
<b>Troubleshooting.....</b>	<b>217</b>
31.1 Power, Hardware Connections, and LEDs .....	217
31.2 NBG-419N Access and Login .....	218
31.3 Internet Access .....	220
31.4 Resetting the NBG-419N to Its Factory Defaults .....	221
31.5 Wireless Router/AP Troubleshooting .....	222
<b>Chapter 32</b>	
Chapter 32 Product Specifications.....	225
32.1 Wall-mounting Instructions .....	228
<b>Part VI: Appendices and Index .....</b>	<b>231</b>
Appendix A Pop-up Windows, JavaScripts and Java Permissions.....	233
Appendix B IP Addresses and Subnetting .....	241
Appendix C Setting up Your Computer's IP Address.....	251
32.1.1 Verifying Settings .....	268
Appendix D Wireless LANs .....	269
32.1.2 WPA(2)-PSK Application Example .....	279
32.1.3 WPA(2) with RADIUS Application Example .....	279
Appendix E Common Services.....	281
Appendix F Legal Information .....	285
<b>Index.....</b>	<b>293</b>

---

# PART I

## Introduction

---

Getting to Know Your NBG-419N (21)

Connection Wizard (25)

Introducing the Web Configurator (37)

NBG-419N Modes (49)

Monitor (43)

Tutorials (89)

Company Confidential

# Getting to Know Your NBG-419N

## 1.1 Overview

This chapter introduces the main features and applications of the NBG-419N.

The NBG-419N extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.

A range of services such as a firewall and content filtering are also available for secure Internet computing. 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).

## 1.2 Applications

You can create the following networks using the NBG-419N:

- **Wired.** You can connect network devices via the Ethernet ports of the NBG-419N so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the NBG-419N to access network resources.
- **WAN.** Connect to a broadband modem/router for Internet access.

Figure 1 NBG-419N Network



## 1.3 Ways to Manage the NBG-419N

Use any of the following methods to manage the NBG-419N.

- Web Configurator. This is recommended for everyday management of the NBG-419N using a (supported) web browser.
- Wireless switch. You can use the built-in switch of the NBG-419N to turn the wireless function on and off without opening the Web Configurator.
- WPS (Wi-Fi Protected Setup) button. You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL Device.

## 1.4 Good Habits for Managing the NBG-419N

Do the following things regularly to make the NBG-419N more secure and to manage the NBG-419N 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 NBG-419N to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG-419N. You could simply restore your last configuration.






## 1.5 LEDs

Figure 2 Front Panel



The following table describes the LEDs and the WPS button.

**Table 1** Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	The NBG-419N is receiving power and functioning properly.
		Off	The NBG-419N is not receiving power.
WLAN 	Green	On	The NBG-419N is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG-419N is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
WPS 	Green	On	WPS is enabled.
		Blinking	The NBG-419N is negotiating a WPS connection with a wireless client.
		Off	The wireless LAN is not ready or has failed.
WAN 	Green	On	The NBG-419N has a successful 10/100MB WAN connection.
		Blinking	The NBG-419N is sending/receiving data through the WAN.
		Off	The WAN connection is not ready, or has failed.
LAN 1-4 	Green	On	The NBG-419N has a successful 10/100MB Ethernet connection.
		Blinking	The NBG-419N is sending/receiving data through the LAN.
		Off	The LAN is not connected.

Company Confidential



# Connection Wizard

## 2.1 Overview

This chapter provides information on the wizard setup screens in the Web Configurator.

The Web Configurator's wizard setup helps you configure your device to access the Internet. Refer to your ISP for your Internet account information. Leave a field blank if you don't have that information.

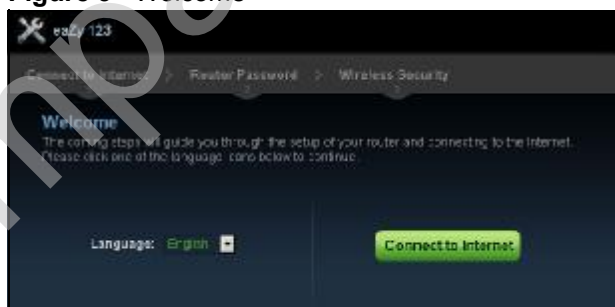
## 2.2 Accessing the Wizard

Launch your web browser and type "http://192.168.1.1" as the website address. Type "1234" (default) as the password and click **Login**.

Note: The Wizard appears when the NBG-419N is accessed for the first time or when you reset the NBG-419N to its default factory settings.

The Wizard screen opens. Choose your **Language** and click **Connect to Internet**.

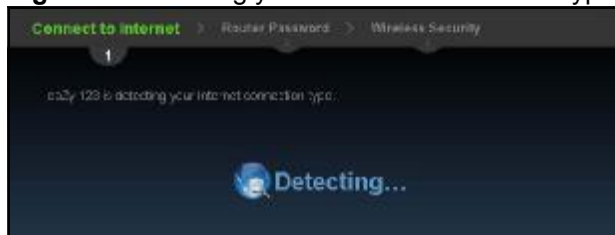
Figure 3 Welcome



## 2.3 Connect to Internet

The NBG-419N offers five Internet connection types. They are **Static IP**, **DHCP**, **PPPoE**, **PPTP** or **L2TP**. The wizard attempts to detect which WAN connection type you are using.

**Figure 4** Detecting your Internet Connection Type

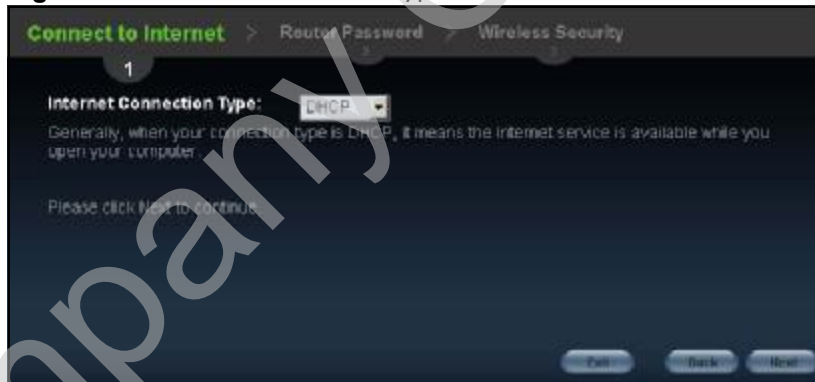


If the wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

Note: If you get an error message, check your hardware connections. Make sure your Internet connection is up and running.

The following screen depends on your Internet connection type. Enter the details provided by your Internet Service Provider (ISP) in the fields (if any).

**Figure 5** Internet Connection Type



Your NBG-419N detects the following Internet Connection type.

**Table 2** Internet Connection Type

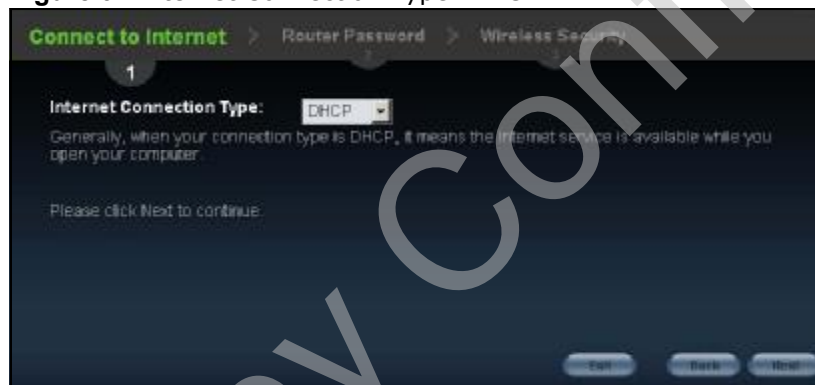
CONNECTION TYPE	DESCRIPTION
Static IP	Select the <b>Static IP</b> if an administrator assigns the IP address of your computer.
DHCP	Select the <b>DHCP</b> (Dynamic Host Configuration Protocol) option when the WAN port is used as a regular Ethernet.

**Table 2** Internet Connection Type

CONNECTION TYPE	DESCRIPTION
PPPoE	Select the <b>PPPoE</b> (Point-to-Point Protocol over Ethernet) option for a dial-up connection.
PPTP	Select the <b>PPTP</b> (Point-to-Point Tunneling Protocol) option for a dial-up connection, and your ISP gave you an IP address and/or subnet mask.
L2TP	Select the <b>L2TP</b> (Layer 2 Tunnel Protocol) if you are connecting to another device over another network (like the Internet or VPN).

### 2.3.1 Connection Type: DHCP

Choose **DHCP** as the **Internet Connection Type** when the WAN port is used as a regular Ethernet. Click **Next**.

**Figure 6** Internet Connection Type: DHCP

Note: If you get an error screen after clicking **Next**, you might have selected the wrong Internet Connection type. Click **Back**, make sure your Internet connection is working and select the right Connection Type. Contact your ISP if you are not sure of your Internet Connection type.

## 2.3.2 Connection Type: Static IP

Choose **Static IP** as the **Internet Connection Type** if your ISP assigned an IP address for your Internet connection. Click **Next**.

**Figure 7** Internet Connection Type: Static IP



The following table describes the labels in this screen.

**Table 3** Internet Connection Type: Static IP

LABEL	DESCRIPTION
Internet Connection Type	Select the <b>Static IP</b> option.
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the IP subnet mask in this field.
Default Gateway	Enter the gateway IP address in this field.
Primary DNS	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 NBG-419N uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server. Enter the primary DNS server's IP address in the fields provided.
Secondary DNS	Enter the secondary DNS server's IP address in the fields provided.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

## 2.3.3 Connection Type: PPPoE

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 NBG-419N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG-419N does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

**Figure 8** Internet Connection Type: PPPoE

The following table describes the labels in this screen.

**Table 4** Internet Connection Type: PPPoE

LABEL	DESCRIPTION
Internet Connection Type	Select the <b>PPPoE</b> option for a dial-up connection.
Dynamic IP	Select this radio button if your ISP did not assign you a fixed IP address.
Static IP	Select this radio button, provided by your ISP to give the NBG-419N a fixed, unique IP address.
IP Address	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.
Exit	Click this to close the wizard screen without saving.

**Table 4** Internet Connection Type: PPPoE

LABEL	DESCRIPTION
Back	Click this to return to the previous screen.
Next	Click this to continue.

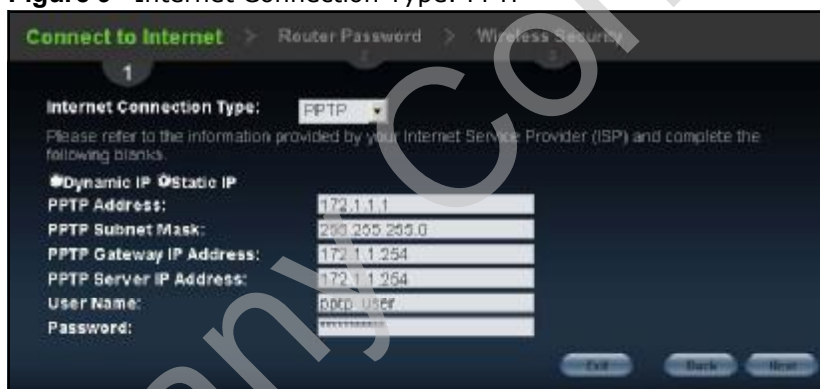
### 2.3.4 Connection Type: PPTP

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 NBG-419N supports one PPTP server connection at any given time.

**Figure 9** Internet Connection Type: PPTP

The following table describes the fields in this screen

**Table 5** Internet Connection Type: PPTP

LABEL	DESCRIPTION
Internet Connection Type	Select <b>PPTP</b> from the drop-down list box. To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
Dynamic IP	Select this radio button if your ISP did not assign you a fixed IP address.
Static IP	Select this radio button, provided by your ISP to give the NBG-419N a fixed, unique IP address.
PPTP Address	Type the (static) IP address assigned to you by your ISP.
PPTP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).

**Table 5** Internet Connection Type: PPTP

LABEL	DESCRIPTION
PPTP Gateway IP Address	Type the gateway IP address of the PPTP server.
PPTP Server IP Address	Type the server IP address of the PPTP server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

### 2.3.5 Connection Type: L2TP

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peer devices over another network (like the Internet).

**Figure 10** Internet Connection Type: L2TP

The following table describes the fields in this screen

**Table 6** Internet Connection Type: L2TP

LABEL	DESCRIPTION
Internet Connection Type	Select <b>L2TP</b> from the drop-down list box.
Dynamic IP	Select this radio button if your ISP did not assign you a fixed IP address.
Static IP	Select this radio button, provided by your ISP to give the NBG-419N a fixed, unique IP address.
L2TP Address	Type the (static) IP address assigned to you by your ISP.
L2TP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).

**Table 6** Internet Connection Type: L2TP

LABEL	DESCRIPTION
L2TP Gateway IP Address	Type the gateway IP address of the L2TP server.
L2TP Server IP Address	Type the server IP address of the L2TP server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

The NBG-419N connects to the Internet.

**Figure 11** Connecting to the Internet

Note: If the Wizard successfully connects to the Internet, it proceeds to the next step. If you get an error message, go back to the previous screen and make sure you have entered the correct information provided by your ISP.



## 2.4 Router Password

Change the login password in the following screen. Enter the new password and retype it to confirm. Click **Next** to proceed with the **Wireless Security** screen.

**Figure 12** Router Password



## 2.5 Wireless Security

Configure Wireless Settings. Configure the wireless network settings on your NBG-419N in the following screen. The fields that show up depend on the kind of security you select.

### 2.5.1 Wireless Security: No Security

Choose **No Security** in the Wireless Security screen to let wireless devices within range access your wireless network.

**Figure 13** Wireless Security: No Security



The following table describes the labels in this screen.

**Table 7** Wireless Security: No Security

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.  If you change this field on the NBG-419N, make sure all wireless stations use the same SSID in order to access the network.
Security mode	Select a <b>Security</b> level from the drop-down list box.  Choose <b>None</b> to have no wireless LAN security configured. If you do not enable any wireless security on your NBG-419N, your network is accessible to any wireless networking device that is within range.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

## 2.5.2 Wireless Security: WPA-PSK/WPA2-PSK

Choose **WPA-PSK** or **WPA2-PSK** security in the Wireless Security screen to set up a password for your wireless network.

**Figure 14** Wireless Security: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

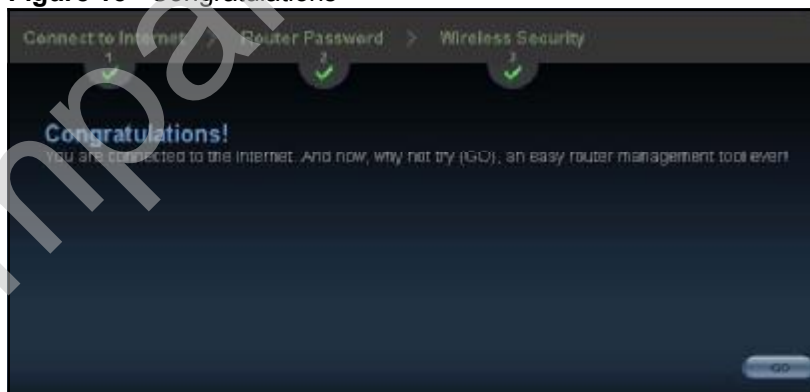
**Table 8** Wireless Security: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.  If you change this field on the NBG-419N, make sure all wireless stations use the same SSID in order to access the network.
Security mode	Select a <b>Security</b> level from the drop-down list box.  Choose <b>WPA-PSK</b> or <b>WPA2-PSK</b> security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK or WPA2-PSK respectively.
Wireless password	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.
Verify Password	Retype the password to confirm.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

Congratulations! Open a web browser, such as Internet Explorer, to visit your favorite website.

**Note:** If you cannot access the Internet when your computer is connected to one of the NBG-419N's LAN ports, check your connections. Then turn the NBG-419N off, wait for a few seconds then turn it back on. If that does not work, log in to the web configurator again and check you have typed all information correctly. See the User's Guide for more suggestions.

**Figure 15** Congratulations



You can also click **ZyGO** to open the **Easy Mode** Web Configurator of your NBG-419N.

You have successfully set up your NBG-419N to operate on your network and access the Internet. You are now ready to connect wirelessly to your NBG-419N and access the Internet.

Company Confidential

# Introducing the Web Configurator

## 3.1 Overview

This chapter describes how to access the NBG-419N Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the NBG-419N 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 ([Chapter 31 on page 217](#)) to see how to make sure these functions are allowed in Internet Explorer.

## 3.2 Accessing the Web Configurator

- 1 Make sure your NBG-419N hardware is properly connected and prepare your computer or computer network to connect to the NBG-419N (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.

### 3.2.1 Login Screen

Note: If this is the first time you are accessing the Web Configurator, you may be redirected to the Wizard. Refer to [Chapter 2 on page 25](#) for the Connection Wizard screens.



The Web Configurator initially displays the following login screen.

**Figure 16** Login screen



The following table describes the labels in this screen.

**Table 9** Login screen

LABEL	DESCRIPTION
Password	Type "1234" (default) as the password.
Language	Select the language you want to use to configure the Web Configurator. Click <b>Login</b> .
	This shows the current weather, either in celsius or fahrenheit, of the city you specify in <a href="#">Section 3.2.3.1 on page 40</a> .
	This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in <a href="#">Section 3.2.3.2 on page 41</a> or <a href="#">Section 26.3 on page 201</a> . The time is in 24-hour format, for example 15:00 is 3:00 PM.

### 3.2.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

**Figure 17** Change Password Screen



The following table describes the labels in this screen.



**Table 10** Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Ignore	Click <b>Ignore</b> if you do not want to change the password this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to [Chapter 24 on page 197](#) to change this). Simply log back into the NBG-419N if this happens.

### 3.2.3 Home Screen

If you have previously logged into the Web Configurator but did not click **Logout**, you may be redirected to the Home screen.

You can also open this screen by clicking **Home** (  Home or  Home ) in the Easy Mode or Expert mode screens.



The Home screen displays as follows.

**Figure 18** Home Screen




The following table describes the labels in this screen.

**Table 11** Home Screen

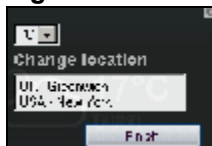
LABEL	DESCRIPTION
Go	Click this to open the Easy mode Web Configurator.
Language	Select a language to go to the Easy mode Web Configurator in that language and click <b>Login</b> .
	(This is just an example). This shows the current weather, either in celsius or fahrenheit, of the city you specify in <a href="#">Section 3.2.3.1 on page 40</a> .
	(This is just an example). This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in <a href="#">Section 3.2.3.2 on page 41</a> or <a href="#">Section 26.3 on page 201</a> .

### 3.2.3.1 Weather Edit

You can change the temperature unit and select the location for which you want to know the weather.

Click the  icon to change the Weather display.

**Figure 19** Change Weather






The following table describes the labels in this screen.

**Table 12** Change Weather

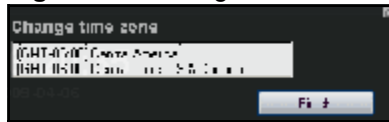
LABEL	DESCRIPTION
°C or °F	Choose which temperature unit you want the NBG-419N to display.
Change Location	Select the location for which you want to know the weather. If the city you want is not listed, choose one that is closest to it.
Finish	Click this to apply the settings and refresh the date and time display.

### 3.2.3.2 Time/Date Edit

One timezone can cover more than one country. You can choose a particular country in which the NBG-419N is located and have the NBG-419N display and use the current time and date for its logs.

Click the  icon to change the Weather display.

**Figure 20** Change Password Screen



The following table describes the labels in this screen.

**Table 13** Change Password Screen

LABEL	DESCRIPTION
Change time zone	Select the specific country whose current time and date you want the NBG-419N to display.
Finish	Click this to apply the settings and refresh the weather display.

Note: You can also edit the timezone in [Section 26.3 on page 201](#).

## 3.3 Resetting the NBG-419N

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 NBG-419N 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 longer than 1 second to restart/reboot the NBG-419N.
- 3 Press the **RESET** button for longer than five seconds to set the NBG-419N back to its factory-default configurations.

## 4.1 Overview

This chapter discusses read-only information related to the device state of the NBG-419N.

Note: To access the Monitor screens, you can also click the links in the Summary table of the Status screen to view the bandwidth consumed, packets sent/received as well as the status of clients connected to the NBG-419N.

## 4.2 What You Can Do

- Use the **BW MGMT Monitor** screen ([Section 4.3 on page 43](#)) to view the amount of network bandwidth that applications running in the network are using.
- Use the **DHCP Table** screen ([Section 4.4 on page 44](#)) to view information related to your DHCP status.
- use the **Packet Statistics** screen ([Section 4.5 on page 45](#)) to view port status, packet specific statistics, the "system up time" and so on.
- Use the **WLAN Station Status** screen ([Section 4.6 on page 46](#)) to view the wireless stations that are currently associated to the NBG-419N.

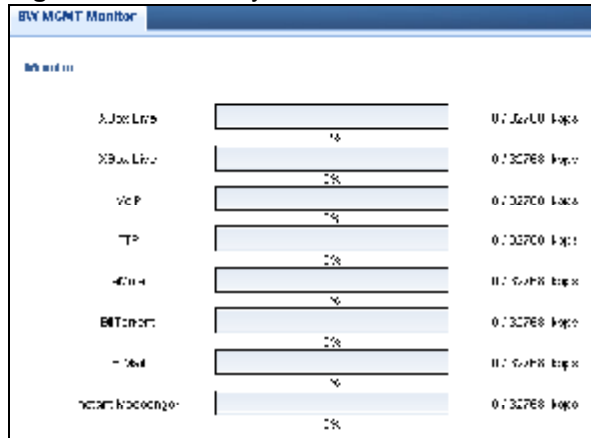
## 4.3 BW MGMT Monitor

The Bandwidth Management (BW MGMT) Monitor allows you to view the amount of network bandwidth that applications running in the network are using.

The bandwidth is measured in kilobits per second (kbps).

The monitor shows what kinds of applications are running in the network, the maximum kbps that each application can use, as well as the percentage of bandwidth it is using.

**Figure 21** Summary: BW MGMT Monitor

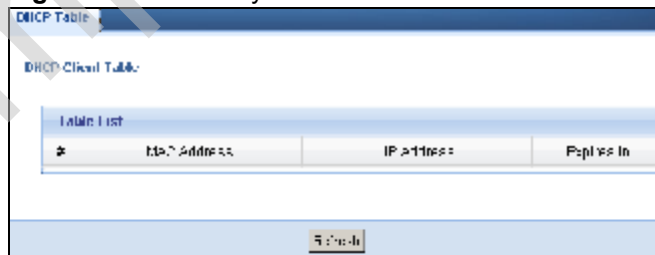


## 4.4 DHCP Table

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 NBG-419N's LAN as a DHCP server or disable it. When configured as a server, the NBG-419N 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 NBG-419N's DHCP server.

**Figure 22** Summary: DHCP Table



The following table describes the labels in this screen.

**Table 14** Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
MAC Address	This field shows the MAC address of the computer with the name in the <b>Host Name</b> field.  Every Ethernet device has a unique MAC (Media Access Control) address 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.
IP Address	This field displays the IP address relative to the # field listed above.
Expires in	This field displays the time when the IP address and MAC address association ends.
Refresh	Click <b>Refresh</b> to renew the screen.

## 4.5 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 23** Summary: Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M	13625	31171	0	1954809	1939482	01:29:11
LAN	100M	13024	7748	0	14250762	873520	01:29:11
WLAN	Down	0	2	0	0	343	00:00:00

System Up Time: 1 hour, 29 mins, 17 secs

Poll Interval(s): 5 sec

The following table describes the labels in this screen.

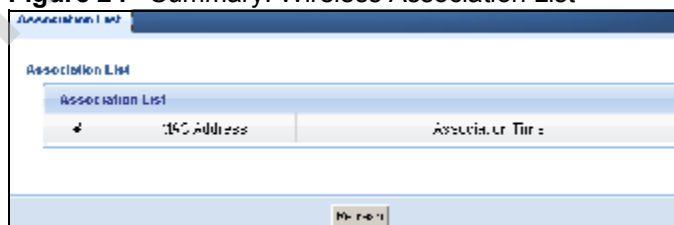
**Table 15** Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG-419N's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or <b>Down</b> when the line is disconnected.  For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays <b>Down</b> when the line is disconnected.  For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and <b>Down</b> when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total time the NBG-419N has been for each session.
System Up Time	This is the total time the NBG-419N has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click <b>Stop</b> to stop refreshing statistics.

## 4.6 WLAN Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the NBG-419N 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 24** Summary: Wireless Association List



The following table describes the labels in this screen.

**Table 16** 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 NBG-419N's WLAN network.
Refresh	Click <b>Refresh</b> to reload the list.

Company Confidential



# NBG-419N Modes

## 5.1 Overview

This chapter introduces the different modes available on your NBG-419N. First, the term “mode” refers to two things in this User’s Guide.

- **Web Configurator mode.** This refers to the Web Configurator interface you want to use for editing NBG-419N features.
- **Device mode.** This is the operating mode of your NBG-419N, or simply how the NBG-419N is being used in the network.

### 5.1.1 Web Configurator Modes

This refers to the configuration interface of the Web Configurator, which has two modes:

- **Easy.** The Web Configurator shows this mode by default. Refer to [Chapter 6 on page 51](#) for more information on the screens in this mode. This interface may be sufficient for users who just want to use the device.
- **Expert.** Advanced users can change to this mode to customize all the functions of the NBG-419N. Click **Expert Mode** after logging into the Web Configurator. The User’s Guide [Chapter 3 on page 37](#) through [Chapter 30 on page 213](#) discusses the screens in this mode.

### 5.1.2 Device Modes

This refers to the operating mode of the NBG-419N, which can act as a:

- **Router.** This is the default device mode of the NBG-419N. Use this mode to connect the local network to another network, like the Internet. Go to [Section 7.3 on page 64](#) to view the **Status** screen in this mode.
- **Access Point.** Use this mode if you want to extend your network by allowing network devices to connect to the NBG-419N wirelessly. Go to [Section 8.4 on page 74](#) view the **Status** screen in this mode.
- **WISP** mode. Use this mode if there is an existing wireless router or access point in the network to which you want to connect your local network. Go to [Section 9.4 on page 81](#) to view the **Status** screen in this mode.

The following figure is a simple illustration of the device configuration modes of the NBG-419N.

**Figure 25** Device Mode Example



For more information on these modes and to change the mode of your NBG-419N, refer to [Chapter 30 on page 213](#).

The menu for changing device modes is available in **Expert** mode only.

Note: Choose your Device Mode carefully to avoid having to change it later.

When changing to another mode, the IP address of the NBG-419N changes. The running applications and services of the network devices connected to the NBG-419N can be interrupted.

In WISP mode, you should know the SSID and wireless security details of the access point to which you want to connect.

# 6

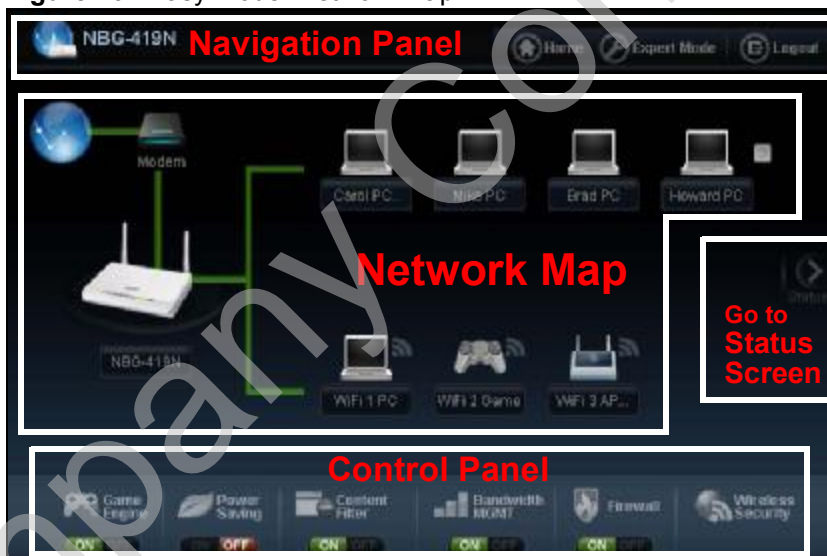
## Easy Mode

### 6.1 Overview

The Web Configurator is set to **Easy Mode** by default. You can configure several key features of the NBG-419N in this mode. This mode is useful to users who are not fully familiar with some features that are usually intended for network administrators.

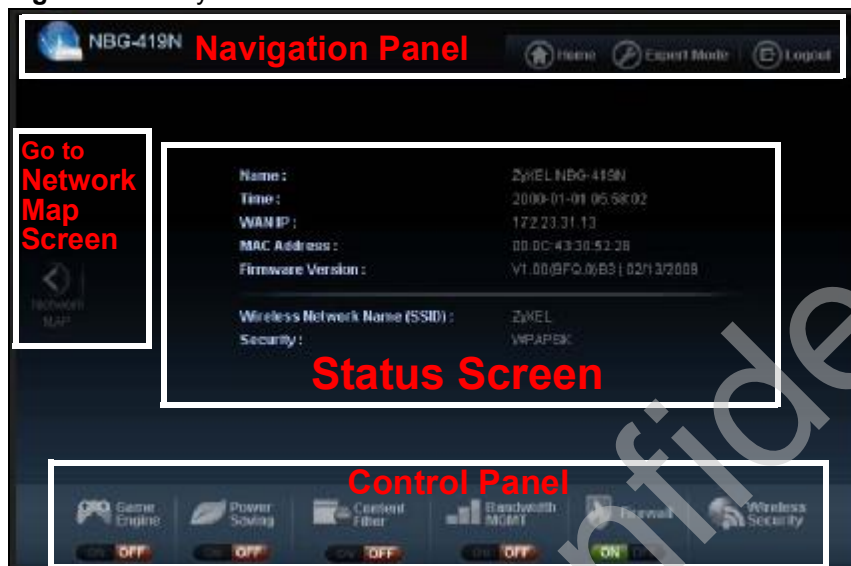
When you log in to the Web Configurator, the following screen opens.

**Figure 26** Easy Mode: Network Map



Click **Status** to open the following screen screen.

**Figure 27** Easy Mode: Status Screen



## 6.2 What You Can Do

You can do the following in this mode:

- Use this **Navigation Panel** (Section 6.4 on page 53) to opt out of the **Easy** mode.
- Use the **Network Map** screen (Section 6.5 on page 53) to check if your NBG-419N can ping the gateway and whether it is connected to the Internet.
- Use the **Control Panel** (Section 6.6 on page 54) to configure and enable NBG-419N features, including wireless security, wireless scheduling and bandwidth management and so on.
- Use the **Status Screen** screen (Section 6.7 on page 61) to view read-only information about the NBG-419N, including the WAN IP, MAC Address of the NBG-419N and the firmware version.

## 6.3 What You Need to Know

Between the different device modes, the Control Panel (Section 6.6 on page 54) changes depending on which features are applicable to the mode:

- **Router Mode:** All Control Panel features are available.

- **Access Point Mode:** Only **Power Saving** and **Wireless Security** are available.
- **WISP Mode:** The available features for this mode are **Game Console**, **Content Filter**, **Bandwidth MGMT**, and **Firewall**.

## 6.4 Navigation Panel

Use this navigation panel to opt out of the **Easy** mode.

**Figure 28** Control Panel



The following table describes the labels in this screen.

**Table 17** Control Panel

ITEM	DESCRIPTION
Home	Click this to go to the <b>Login</b> page.
Expert Mode	Click this to change to <b>Expert</b> mode and customize features of the NBG-419N.
Logout	Click this to end the Web Configurator session.

## 6.5 Network Map

**Note:** The Network MAP is viewable by Windows XP (need to install patch), Windows Vista and Windows 7 users only. For Windows XP (Service Pack 2) users, you can see the network devices connected to the NBG-419N by downloading the LLTD (Link Layer Topology Discovery) patch from the Microsoft Website.

**Note:** Don't worry if the Network Map does not display in your web browser. This feature may not be supported by your system. You can still configure the Control Panel ([Section 6.6 on page 54](#)) in the Easy Mode and the NBG-419N features that you want to use in the Expert Mode.

When you log into the Network Configurator, the Network Map is shown as follows.

**Figure 29** Network Map



The line connecting the NBG-419N to the gateway becomes green when the NBG-419N is able to ping the gateway. It becomes red when the ping initiating from the NBG-419N does not get a response from the gateway. The same rule applies to the line connecting the gateway to the Internet.

You can also view the devices (represented by icons indicating the kind of network device) connected to the NBG-419N, including those connecting wirelessly. Right-click on the NBG-419N icon to refresh the network map and go to the Wizard. Right click on the other icons to view information about the device.

## 6.6 Control Panel

The features configurable in **Easy Mode** are shown in the **Control Panel**.

**Figure 30** Control Panel



Switch **ON** to enable the feature. Otherwise, switch **OFF**. If the feature is turned on, the green light flashes. If it is turned off, the red light flashes.

Additionally, click the feature to open a screen where you can edit its settings.

The following table describes the labels in this screen.

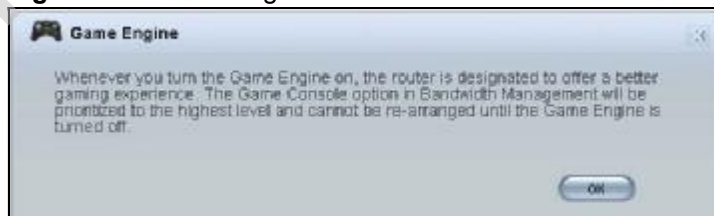
**Table 18** Control Panel

ITEM	DESCRIPTION
Game Engine	Switch <b>ON</b> to maximize bandwidth for gaming traffic in your network. Otherwise, switch <b>OFF</b> . Refer to <a href="#">Section 6.6.1 on page 55</a> to see this screen.
Power Saving	Click this to schedule the wireless feature of the NBG-419N. Disabling the wireless function helps lower the energy consumption of the NBG-419N. Switch <b>ON</b> to apply wireless scheduling. Otherwise, switch <b>OFF</b> . Refer to <a href="#">Section 6.6.2 on page 56</a> to see this screen.
Content Filter	Click this to restrict access to certain websites, based on keywords contained in URLs, to which you do not want users in your network to open. Switch <b>ON</b> to apply website filtering. Otherwise, switch <b>OFF</b> . Refer to <a href="#">Section 6.6.3 on page 57</a> to see this screen.
Bandwidth Mgmt	Click this to edit bandwidth management for predefined applications. Switch <b>ON</b> to have the NBG-419N management bandwidth for uplink and downlink traffic according to an application or service. Otherwise, switch <b>OFF</b> . Refer to <a href="#">Section 6.6.4 on page 58</a> to see this screen.
Firewall	Switch <b>ON</b> to ensure that your network is protected from Denial of Service (DoS) attacks. Otherwise, switch <b>OFF</b> . Refer to <a href="#">Section 6.6.5 on page 58</a> to see this screen.
Wireless Security	Click this to configure the wireless security, such as SSID, security mode and WPS key on your NBG-419N. Refer to <a href="#">Section 6.6.6 on page 59</a> to see this screen.

## 6.6.1 Game Engine

When this feature is enabled, the NBG-419N maximizes the bandwidth for gaming traffic that it forwards out through an interface.

**Figure 31** Game Engine



Note: When this is switched on, the **Game Console** tab in the **Bandwidth Mgmt** screen is automatically positioned on top.

Turn this off if your network is not using gaming.

Click **OK** to close this screen.

## 6.6.2 Power Saving

Use this screen to set the day of the week and time of the day when your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default.

Disabling the wireless capability lowers the energy consumption of the of the NBG-419N.

**Figure 32** Power Saving



The following table describes the labels in this screen.

**Table 19** Power Saving

LABEL	DESCRIPTION
WLAN Status	Select <b>On</b> or <b>Off</b> to specify whether the Wireless LAN is turned on or off (depending on what you selected in the <b>WLAN Status</b> field). This field works in conjunction with the <b>Day</b> and <b>Except for the following times</b> fields.
Day	Select <b>Everyday</b> or the specific days to turn the Wireless LAN on or off.  If you select <b>Everyday</b> you can not select any specific days. This field works in conjunction with the <b>Except for the following times</b> field.

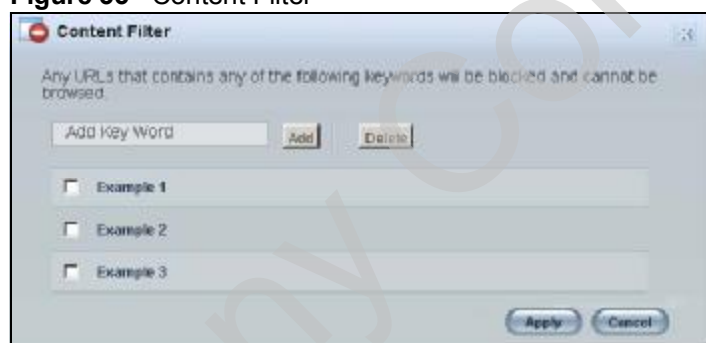


**Table 19** Power Saving

LABEL	DESCRIPTION
For the following times (24-Hour Format)	Select a begin time using the first set of <b>hour</b> and minute ( <b>min</b> ) drop down boxes and select an end time using the second set of <b>hour</b> and minute ( <b>min</b> ) drop down boxes. If you have chosen <b>On</b> earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen <b>Off</b> earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.  In this time format, midnight is 00:00 and progresses up to 24:00. For example, 6:00 PM is 18:00.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 6.6.3 Content Filter

Use this screen to restrict access to certain websites, based on keywords contained in URLs, to which you do not want users in your network to open.

**Figure 33** Content Filter

The following table describes the labels in this screen.

**Table 20** Content Filter

LABEL	DESCRIPTION
Add	Click <b>Add</b> after you have typed a keyword.  Repeat this procedure to add other keywords. Up to 64 keywords are allowed.  Note: The NBG-419N does not recognize wildcard characters as keywords.  When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the text box and click <b>Delete</b> to remove it. The keyword disappears from the text box after you click <b>Apply</b> .

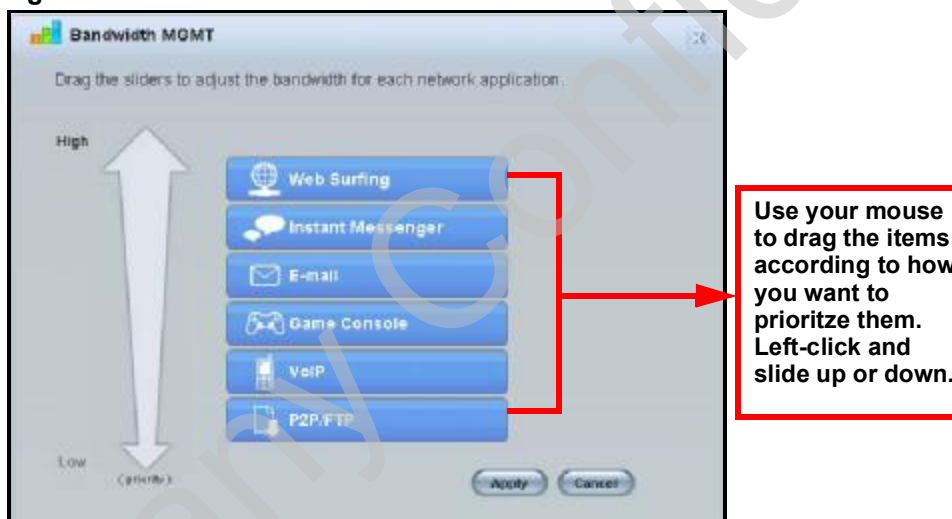
**Table 20** Content Filter

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to close this screen without saving any changes.

## 6.6.4 Bandwidth MGMT

Use this screen to set bandwidth allocation to pre-defined services and applications for bandwidth allocation.

The NBG-419N uses bandwidth management for incoming and outgoing traffic. Rank the services and applications by dragging them accordingly from **High** to **Low** and click **Apply**. Click **Cancel** to close the screen.

**Figure 34** Bandwidth MGMT

## 6.6.5 Firewall

Enable this feature to protect the network from Denial of Service (DoS) attacks. The NBG-419N blocks repetitive pings from the WAN that can otherwise cause systems to slow down or hang.

**Figure 35** Firewall

Click **OK** to close this screen.

## 6.6.6 Wireless Security

Use this screen to configure security for your the Wireless LAN. You can enter the SSID and select the wireless security mode in the following screen.

Note: You can enable the Wireless function of your NBG-419N by first turning on the switch in the back panel.

**Figure 36** Wireless Security



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

**Table 21** Wireless Security

LABEL	DESCRIPTION
Wireless Network 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 keyboard characters) for the wireless LAN.  The default SSID is NBG-419N.
Security mode	Select <b>WPA-PSK</b> or <b>WPA2-PSK</b> 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.  Select <b>No Security</b> to allow any client to connect to this network without authentication.
Wireless password	This field appears when you choose wither <b>WPA-PSK</b> or <b>WPA2-PSK</b> as the security mode.  Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Verify password	Type the password again to confirm.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Cancel	Click <b>Cancel</b> to close this screen.
WPS	Click this to configure the WPS screen.  You can transfer the wireless settings configured here ( <b>Wireless Security</b> screen) to another wireless device that supports WPS.

## 6.6.7 WPS

Use this screen to add a wireless station to the network using WPS. Click **WPS** in the **Wireless Security** to open the following screen.

**Figure 37** Wireless Security: WPS



The following table describes the labels in this screen.

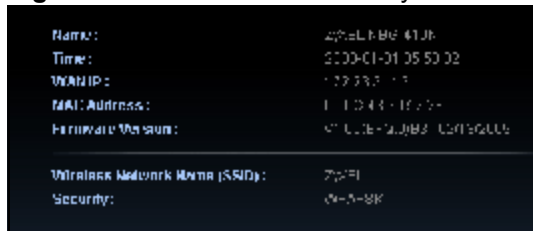
**Table 22** Wireless Security: WPS

LABEL	DESCRIPTION
Wireless Security	Click this to go back to the Wireless Security screen.
WPS	<p>Create a secure wireless network simply by pressing a button. The NBG-419N scans for a WPS-enabled device within the range and performs wireless security information synchronization.</p> <p><b>Note:</b> After you click the <b>WPS</b> button on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.</p>
Register	<p>Create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG-419N's interface and pushing this button.</p> <p>Type the same PIN number generated in the wireless station's utility. Then click <b>Register</b> to associate to each other and perform the wireless security information synchronization.</p>
Exit	Click <b>Exit</b> to close this screen.

## 6.7 Status Screen in Easy Mode

In the Network Map screen, click **Status** to view read-only information about the NBG-419N.

**Figure 38** Status Screen in Easy Mode



The following table describes the labels in this screen.

**Table 23** Status Screen in Easy Mode

ITEM	DESCRIPTION
Name	This is the name of the NBG-419N in the network. You can change this in the <b>Maintenance &gt; General</b> screen in <a href="#">Section 24.3 on page 197</a> .
Time	This is the current system date and time. The date is in YYYY:MM:DD (Year-Month-Day) format. The time is in HH:MM:SS (Hour:Minutes:Seconds) format.
WAN IP	This is the IP address of the WAN port.
MAC Address	This is the MAC address of the NBG-419N.
Firmware Version	This shows the firmware version of the NBG-419N. The firmware version format shows the trunk version, model code and release number.
Wireless Network Name	This shows the SSID of the wireless network. You can configure this in the Wireless Security screen ( <a href="#">Section 6.6.6 on page 59</a> ; <a href="#">Section 11.3.1.1 on page 101</a> ).
Security	This shows the wireless security used by the NBG-419N.

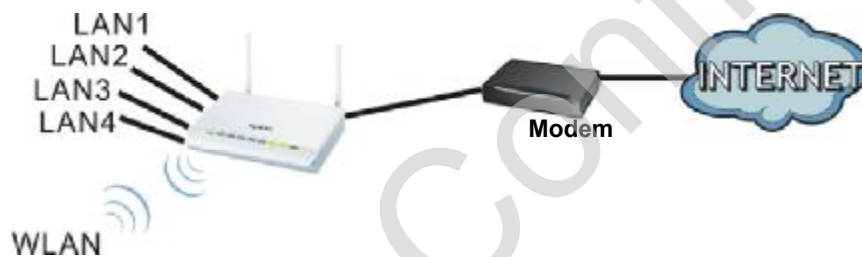
Company Confidential

## Router Mode

### 7.1 Overview

The NBG-419N is set to router mode by default. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the NBG-419N connects the local network (**LAN1 ~ LAN4**) to the Internet.

**Figure 39** NBG-419N Network




Note: The Status screen is shown after changing to the Expert mode of the Web Configurator. It varies depending on the device mode of your NBG-419N.

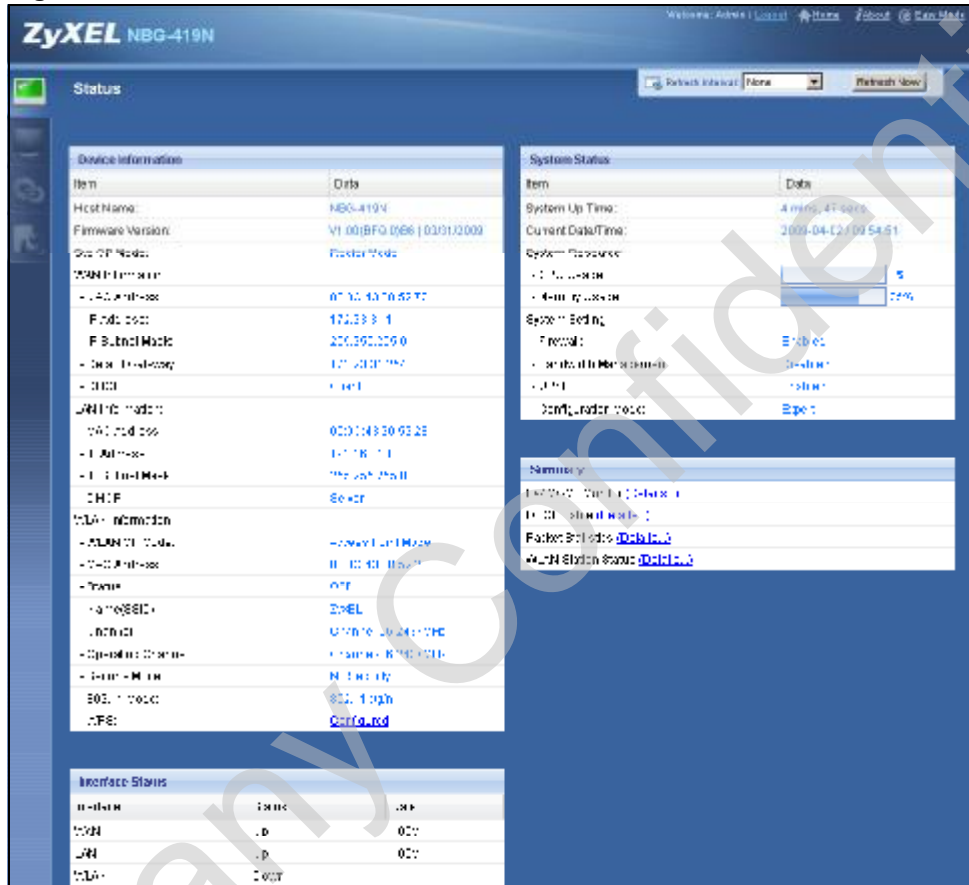
### 7.2 What You Can Do

Use the **Status** screen ([Section 7.3 on page 64](#)) to view read-only information about your NBG-419N.

## 7.3 Status Screen





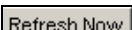
Click  to open the status screen.

**Figure 40** Status Screen: Router Mode







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

**Table 24** Status Screen Icon Key: Router Mode

ICON	DESCRIPTION
	Click this icon to view copyright and a link for related product information.
	Click this icon to go to Easy Mode. See <a href="#">Chapter 6 on page 51</a> .
	Click this to go to the Home page. See <a href="#">Chapter 4 on page 43</a> .
	Select a number of seconds or <b>None</b> from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.



**Table 24** Status Screen Icon Key: Router Mode (continued)

ICON	DESCRIPTION
	Click this icon to see the Status page. The information in this screen depends on the device mode you select.
	Click this icon to see the <b>Monitor</b> navigation menu.
	Click this icon to see the <b>Configuration</b> navigation menu.
	Click this icon to see the <b>Maintenance</b> navigation menu.

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

**Table 25** Status Screen: Router Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the <b>System Name</b> you enter in the <b>Maintenance &gt; General</b> screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode ( <a href="#">Section 5.1.2 on page 49</a> ) to which the NBG-419N is set - <b>Router Mode</b> .
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.
- Default Gateway	This shows the WAN port's gateway IP address.
- DHCP	This shows the LAN port's DHCP role - <b>Client</b> or <b>Server</b> .
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - <b>Server</b> or <b>None</b> .
WLAN Information	
- WLAN OP Mode	This is the device mode ( <a href="#">Section 5.1.2 on page 49</a> ) to which the NBG-419N's wireless LAN is set - <b>Access Point Mode</b> .
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - <b>ON</b> or <b>OFF</b> .
- Name (SSID)	This shows a descriptive name used to identify the NBG-419N in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG-419N is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG-419N is using.

**Table 25** Status Screen: Router Mode

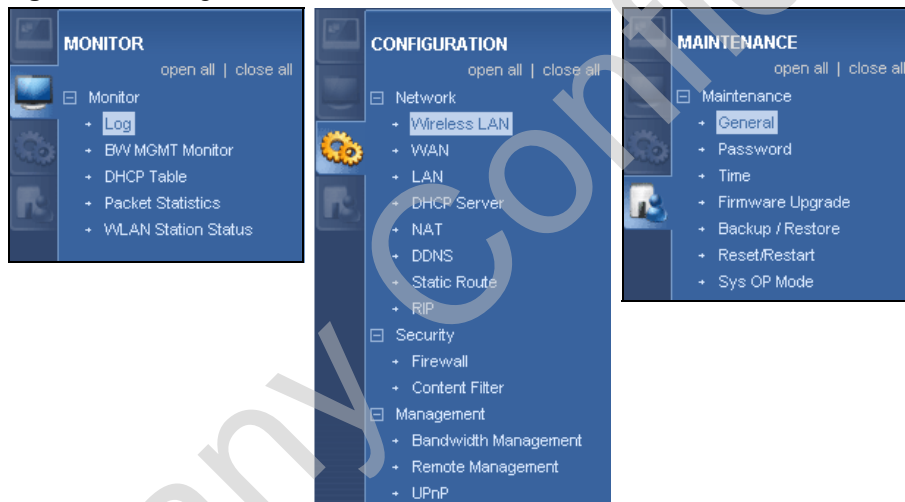
LABEL	DESCRIPTION
- 802.11 Mode	This shows the wireless standard.
- WPS	This displays <b>Configured</b> when the WPS has been set up. This displays <b>Unconfigured</b> if the WPS has not been set up. Click the status to display <b>Network &gt; Wireless LAN &gt; WPS</b> screen.
System Status	
Item	This column shows the type of data the NBG-419N is recording.
Data	This column shows the actual data recorded by the NBG-419N.
System Up Time	This is the total time the NBG-419N has been on.
Current Date/Time	This field displays your NBG-419N's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG-419N's processing ability is currently used. When this percentage is close to 100%, the NBG-419N 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 NBG-419N is using.
System Setting	
- Firewall	This shows whether the firewall is enabled or not.
- Bandwidth Management	This shows whether the bandwidth management is enabled or not.
- UPnP	This shows whether UPnP is enabled or not.
- Configuration Mode	This shows the web configurator mode you are viewing - <b>Expert</b> .
Interface Status	
Interface	This displays the NBG-419N port types. The port types are: <b>WAN</b> , <b>LAN</b> and <b>WLAN</b> .
Status	For the LAN and WAN ports, this field displays <b>Down</b> (line is down) or <b>Up</b> (line is up or connected). For the WLAN, it displays <b>Up</b> when the WLAN is enabled or <b>Down</b> when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or <b>N/A</b> when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays <b>N/A</b> when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and <b>N/A</b> when the WLAN is disabled.
Summary	
BW MGMT Monitor	Click <b>Details...</b> to go to the <b>Monitor &gt; BW MGMT Monitor</b> screen ( <a href="#">Section 4.3 on page 43</a> ). Use this screen to view the amount of network bandwidth that applications running in the network are using.

**Table 25** Status Screen: Router Mode

LABEL	DESCRIPTION
DHCP Table	Click <b>Details...</b> to go to the <b>Monitor &gt; DHCP Table</b> screen (Section 4.4 on page 44). Use this screen to view current DHCP client information.
Packet Statistics	Click <b>Details...</b> to go to the <b>Monitor &gt; Packet Statistics</b> screen (Section 4.5 on page 45). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click <b>Details...</b> to go to the <b>Monitor &gt; WLAN Station Status</b> screen (Section 4.6 on page 46). Use this screen to view the wireless stations that are currently associated to the NBG-419N.

### 7.3.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG-419N features.

**Figure 41** Navigation Panel: Router Mode

The following table describes the sub-menus.

**Table 26** Navigation Panel: Router Mode

LINK	TAB	FUNCTION
Status		This screen shows the NBG-419N's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
<b>MONITOR</b>		
Log		Use this screen to view the list of activities recorded by your NBG-419N.
BW MGMT		Use this screen to view the amount of network bandwidth that applications running in the network are using.
DHCP Table		Use this screen to view current DHCP client information.

**Table 26** Navigation Panel: Router Mode

LINK	TAB	FUNCTION
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 NBG-419N.
<b>CONFIGURATION</b>		
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG-419N to block access to devices or block the devices from accessing the NBG-419N.
	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.
	WDS	Use this screen to set up Wireless Distribution System (WDS) on your NBG-419N.
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.
	IGMP Snooping	Use this screen to enable IGMP snooping if you have LAN users that subscribe to multicast services.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to have the NBG-419N apply IP alias to create LAN subnets.
DHCP Server	General	Use this screen to enable the NBG-419N'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.
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the NBG-419N.
	Advanced	Use this screen to change your NBG-419N's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS.
Static Route	IP Static Route	Use this screen to configure IP static routes.

**Table 26** Navigation Panel: Router Mode

LINK	TAB	FUNCTION
RIP		Use this screen to enable RIPv1 or RIPv2, which are LAN broadcast protocols.
<b>Security</b>		
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		Use this screen to block certain web features and sites containing certain keywords in the URL.
<b>Management</b>		
Bandwidth Management	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 amount of network bandwidth that applications running in the network are using.
Remote Management	WWW	Use this screen to be able to access the NBG-419N from the LAN, WAN or both.
UPnP	General	Use this screen to enable UPnP on the NBG-419N.
<b>MAINTENANCE</b>		
General		Use this screen to view and change administrative settings such as system and domain names.
Password	Password Setup	Use this screen to change the password of your NBG-419N.
Time	Time Setting	Use this screen to change your NBG-419N's time and date.
Remote Management	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG-419N.
Firmware Upgrade		Use this screen to upload firmware to your NBG-419N.
Backup/Restore		Use this screen to backup and restore the configuration or reset the factory defaults to your NBG-419N.
Reset/Restart	Restart	This screen allows you to reboot the NBG-419N without turning the power off.
Sys OP Mode		This screen allows you to select whether your device acts as a Router or a Access Point.

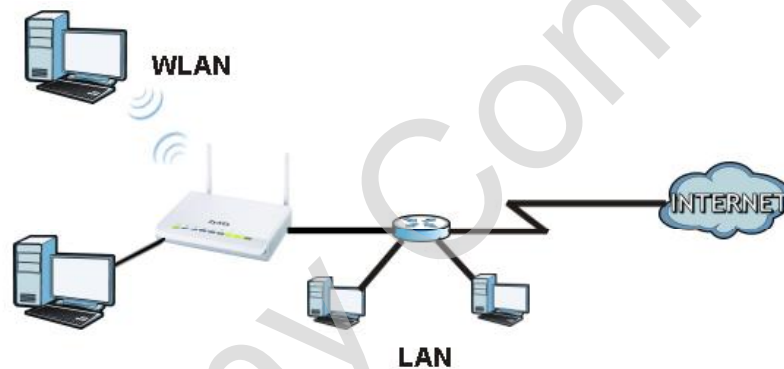
Company Confidential

# Access Point Mode

## 8.1 Overview

Use your NBG-419N as an access point (AP) if you already have a router or gateway on your network. In this mode your NBG-419N bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

**Figure 42** Wireless Internet Access in Access Point Mode



Many screens that are available in Router mode are not available in Access Point mode, such as bandwidth management and firewall.

Note: See [Chapter 10 on page 89](#) for an example of setting up a wireless network in Access Point mode.

## 8.2 What You Can Do

- Use the **Status** screen ([Section 8.4 on page 74](#)) to view read-only information about your NBG-419N.
- Use the **LAN** screen ([Section 8.5 on page 76](#)) to set the IP address for your NBG-419N acting as an access point.

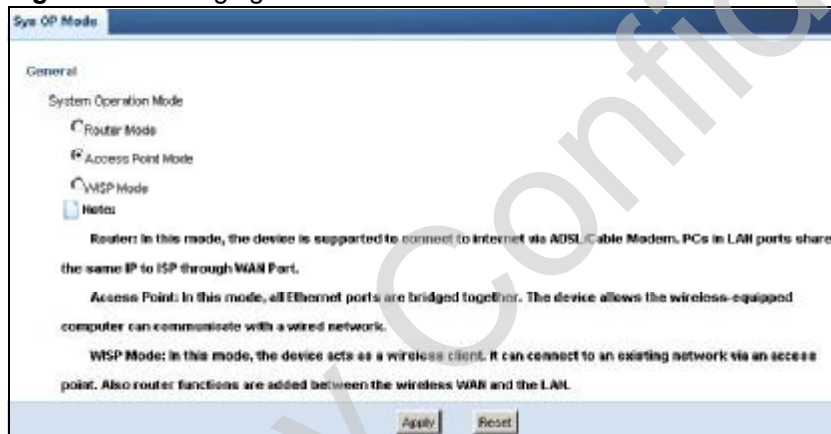
## 8.3 What You Need to Know

See [Chapter 10 on page 89](#) for a tutorial on setting up a network with the NBG-419N as an access point.

### 8.3.1 Setting your NBG-419N 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 use your NBG-419N as an access point, go to **Maintenance > Sys OP Mode > General** and select **Access Point mode**.

**Figure 43** Changing to Access Point mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG-419N is already in Access Point mode.

- 3 When you select **Access Point Mode**, the following pop-up message window appears.

**Figure 44** Pop up for Access Point mode



Click **OK**. The Web Configurator refreshes once the change to Access Point mode is successful.



### 8.3.2 Accessing the Web Configurator in Access Point Mode

Log in to the Web Configurator in Access Point mode, do the following:

- 1 Connect your computer to the LAN port of the NBG-419N.
- 2 The default IP address of the NBG-419N is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix C on page 251](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.


Note: After clicking Login, the Easy mode appears. Refer to [Section on page 51](#) for the Easy mode screens. Change to Expert mode to see the screens described in the sections following this.

### 8.3.3 Configuring your WLAN, Bandwidth Management and Maintenance Settings

The configuration of wireless, bandwidth management and maintenance settings in **Access Point** mode is the same as for **Router Mode**.

- See [Chapter 11 on page 99](#) for information on the configuring your wireless network.
- See [Chapter 21 on page 173](#) for information on configuring your Bandwidth Management screen.
- See [Maintenance and Troubleshooting \(195\)](#) for information on configuring your Maintenance settings.

## 8.4 AP Mode Status Screen

Click  to open the **Status** screen.

**Figure 45** Status Screen: Access Point Mode



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

**Table 27** Status Screen: Access Point Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the <b>System Name</b> you enter in the <b>Maintenance &gt; General</b> screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode ( <a href="#">Section 5.1.2 on page 49</a> ) to which the NBG-419N is set - <b>Access Point Mode</b> .
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - <b>Server, Client or None</b> .

**Table 27** Status Screen: Access Point Mode

LABEL	DESCRIPTION
WLAN Information	
- WLAN OP Mode	This is the device mode ( <a href="#">Section 5.1.2 on page 49</a> ) to which the NBG-419N's wireless LAN is set - <b>Access Point Mode</b> .
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - <b>ON</b> or <b>OFF</b> .
- Name (SSID)	This shows a descriptive name used to identify the NBG-419N in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG-419N is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG-419N is using.
- 802.11 Mode	This shows the wireless standard.
- WPS	This displays <b>Configured</b> when the WPS has been set up. This displays <b>Unconfigured</b> if the WPS has not been set up. Click the status to display <b>Network &gt; Wireless LAN &gt; WPS</b> screen.
System Status	
Item	This column shows the type of data the NBG-419N is recording.
Data	This column shows the actual data recorded by the NBG-419N.
System Up Time	This is the total time the NBG-419N has been on.
Current Date/Time	This field displays your NBG-419N's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG-419N's processing ability is currently used. When this percentage is close to 100%, the NBG-419N 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 NBG-419N is using.
System Setting	
- Configuration Mode	This shows the web configurator mode you are viewing - <b>Expert</b> .
Interface Status	
Interface	This displays the NBG-419N port types. The port types are: <b>LAN</b> and <b>WLAN</b> .
Status	For the LAN and WAN ports, this field displays <b>Down</b> (line is down) or <b>Up</b> (line is up or connected). For the WLAN, it displays <b>Up</b> when the WLAN is enabled or <b>Down</b> when the WLAN is disabled.

**Table 27** Status Screen: Access Point Mode

LABEL	DESCRIPTION
Rate	<p>For the LAN ports, this displays the port speed and duplex setting or <b>N/A</b> when the line is disconnected.</p> <p>For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays <b>N/A</b> when the line is disconnected.</p> <p>For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and <b>N/A</b> when the WLAN is disabled.</p>
Summary	
Packet Statistics	Click <b>Details...</b> to go to the <b>Monitor &gt; Packet Statistics</b> screen (Section 4.5 on page 45). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click <b>Details...</b> to go to the <b>Monitor &gt; WLAN Station Status</b> screen (Section 4.6 on page 46). Use this screen to view the wireless stations that are currently associated to the NBG-419N.

### 8.4.0.1 Navigation Panel

Use the menu in the navigation panel to configure NBG-419N features in Access Point mode.

The following screen and table show the features you can configure in Access Point mode.

**Figure 46** Menu: Access Point Mode

Refer to [Table 26 on page 67](#) for descriptions of the labels shown in the **Navigation** panel.

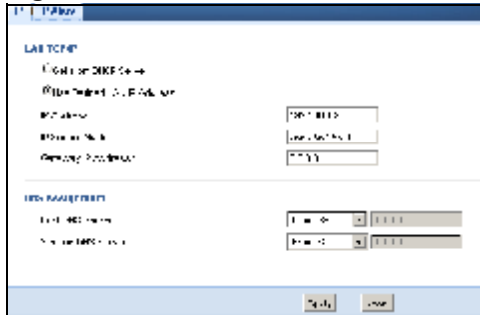
## 8.5 LAN Screen

Use this section to configure your LAN settings while in **Access Point** mode.

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

Note: If you change the IP address of the NBG-419N in the screen below, you will need to log into the NBG-419N again using the new IP address.

**Figure 47** Network > LAN > IP



The table below describes the labels in the screen.

**Table 28** Network > LAN > IP

LABEL	DESCRIPTION
Get from DHCP Server	<p>Click this to deploy the NBG-419N as an access point in the network.</p> <p>When you enable this, the NBG-419N gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the NBG-419N can now access the network (i.e., the Internet if the IP address is given by the ISP).</p> <p>The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the NBG-419N. You need to reset the NBG-419N to be able to access the Web Configurator again (see <a href="#">Section 28.3 on page 208</a> for details on how to reset the NBG-419N).</p> <p>Also when you select this, you cannot enter an IP address for your NBG-419N in the field below.</p>
Use Defined LAN IP Address	Click this if you want to specify the IP address of your NBG-419N. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.2. 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 NBG-419N 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 NBG-419N.
Gateway IP Address	Enter a <b>Gateway IP Address</b> (if your ISP or network administrator gave you one) in this field.
DNS Assignment	

LABEL	DESCRIPTION
First DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the NBG-419N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
Second DNS Server	Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> .  Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click <b>Apply</b> to save your changes to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## WISP Mode

### 9.1 Overview

Your NBG-419N can act as a wireless client. In wireless client mode, it can connect to an existing network via an access point. Use this mode if you already have an access point or router in your network.

In the example below, one NBG-419N (**A**) is configured as a wireless client and another is used as an access point (**B**). The wireless client has two clients that need to connect to the Internet. The NBG-419N wirelessly connects to the available access point (**B**).

**Figure 48** Wireless Client Mode



After the NBG-419N and the access point connect, the NBG-419N acquires its WAN IP address from the access point. The clients of the NBG-419N can now surf the Internet.

### 9.2 What You Can Do

- Use the **Status** screen ([Section 8.4 on page 74](#)) to view read-only information about your NBG-419N.
- Use the **LAN** screen ([Section 8.5 on page 76](#)) to set the IP address for your NBG-419N acting as an access point.
- Use the **Wireless LAN** screen ( ) to associate your NBG-419N (acting as a wireless client) with an existing access point.

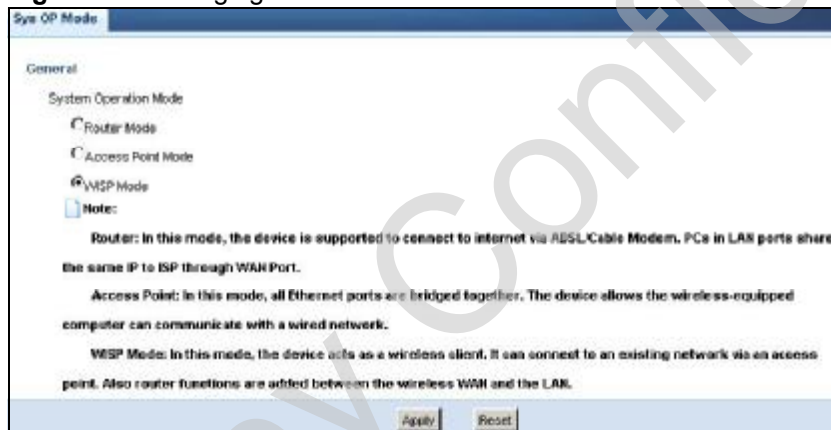
## 9.3 What You Need to Know

With the exception of the **LAN** screen, the **Monitor**, **Configuration** and **Maintenance** screens in WISP mode are similar to the ones in Router Mode. See [Chapter 11 on page 99](#) through [Chapter 30 on page 213](#) of this User's Guide.

### 9.3.1 Setting your NBG-419N to WISP 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 NBG-419N to **AP Mode**, go to **Maintenance > Sys OP Mode > General** and select **WISP Mode**.

**Figure 49** Changing to WISP mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG-419N is already in WISP mode.

- 3 When you select **WISP Mode**, the following pop-up message window appears.

**Figure 50** Pop up window for WISP mode



Click **OK**. The Web Configurator refreshes once the change to WISP mode is successful.

### 9.3.2 Accessing the Web Configurator in WISP Mode

To login to Web Configurator in WISP mode, do the following:




- 1 Connect your computer to the LAN port of the NBG-419N.
- 2 The default IP address of the NBG-419N is "192.168.1.1". If you did not change this, you can use the same IP address in WISP mode. Open a web browser such as Internet Explorer and type "192.168.1.1" as the web address in your web browser.

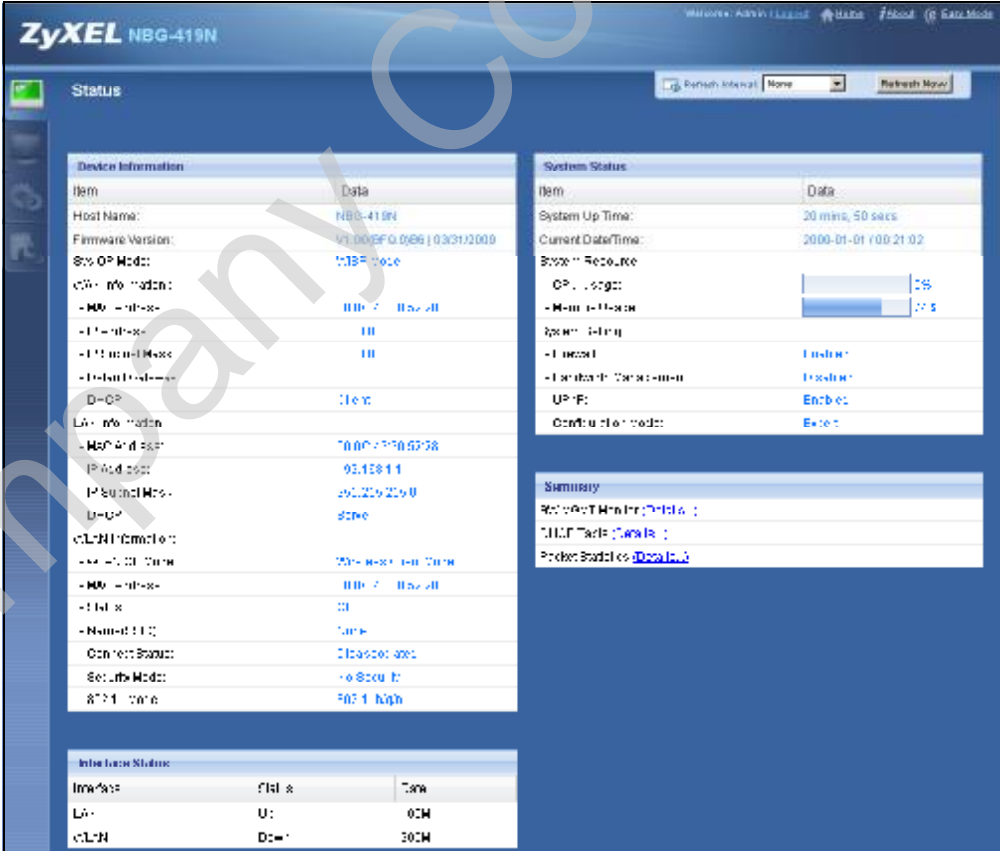
If you changed the IP address of your NBG-419N while in Router Mode, use this IP address in WISP mode. The WISP mode IP address is always the same as the Router mode IP address.

Note: After clicking Login, the Easy mode appears. Refer to [Section on page 51](#) for the Easy mode screens. Click Expert mode to see the screens described in the sections following this.

## 9.4 WISP Mode Status Screen

Click  to open the status screen.

**Figure 51** Status: WISP Mode



The screenshot shows the ZyXEL NBG-419N WISP Mode Status screen. The interface is divided into several sections:

- Device Information:** A table listing various system parameters such as Host Name, Firmware Version, Show OP Mode, CPU Info, Memory, and LAN Info.
- System Status:** A table showing System Up Time, Current DateTime, System Resource (CPU usage, Memory usage), System Setting, and Configuration mode.
- Summary:** A section providing a quick overview of the system's status.
- Interface Statistics:** A table showing statistics for the LAN and WAN interfaces, including links up/down and data transfer rates.

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

**Table 29** Status Screen: WISP Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the <b>System Name</b> you enter in the <b>Maintenance &gt; General</b> screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode ( <a href="#">Section 5.1.2 on page 49</a> ) to which the NBG-419N is set - <b>WISP Mode</b> .
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.
- Default Gateway	This shows the WAN port's gateway IP address.
- DHCP	This shows the LAN port's DHCP role - <b>Client</b> or <b>Server</b> .
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - <b>Server</b> or <b>None</b> .
WLAN Information	
- WLAN OP Mode	This is the device mode ( <a href="#">Section 5.1.2 on page 49</a> ) to which the NBG-419N's wireless LAN is set - <b>Access Point Mode</b> .
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - <b>ON</b> or <b>OFF</b> .
- Name (SSID)	This shows a descriptive name used to identify the NBG-419N in the wireless LAN.
- Connect Status	This shows whether or not the NBG-419N has successfully associated with an access point - <b>Connected</b> or <b>Disassociated</b> .
- Security Mode	This shows the level of wireless security the NBG-419N is using.
- 802.11 Mode	This shows the wireless standard.
System Status	
Item	This column shows the type of data the NBG-419N is recording.
Data	This column shows the actual data recorded by the NBG-419N.
System Up Time	This is the total time the NBG-419N has been on.
Current Date/Time	This field displays your NBG-419N's present date and time.
System Resource	

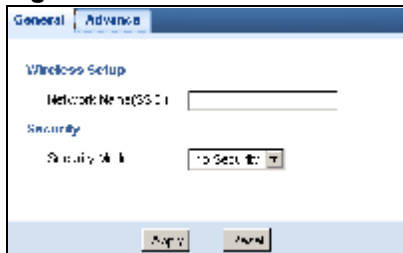
**Table 29** Status Screen: WISP Mode

LABEL	DESCRIPTION
- CPU Usage	This displays what percentage of the NBG-419N's processing ability is currently used. When this percentage is close to 100%, the NBG-419N 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 NBG-419N is using.
System Setting	
- Firewall	This shows whether the firewall is enabled or not.
- Bandwidth Management	This shows whether the bandwidth management is enabled or not.
- UPnP	This shows whether UPnP is enabled or not.
- Configuration Mode	This shows the web configurator mode you are viewing - <b>Expert</b> .
Interface Status	
Interface	This displays the NBG-419N port types. The port types are: <b>LAN</b> and <b>WLAN</b> .
Status	For the LAN and WAN ports, this field displays <b>Down</b> (line is down) or <b>Up</b> (line is up or connected).  For the WLAN, it displays <b>Up</b> when the WLAN is enabled or <b>Down</b> when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or <b>N/A</b> when the line is disconnected.  For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays <b>N/A</b> when the line is disconnected.  For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and <b>N/A</b> when the WLAN is disabled.
Summary	
BW MGMT Monitor	Click <b>Details...</b> to go to the <b>Monitor &gt; BW MGMT Monitor</b> screen ( <a href="#">Section 4.3 on page 43</a> ). Use this screen to view the amount of network bandwidth that applications running in the network are using.
DHCP Table	Click <b>Details...</b> to go to the <b>Monitor &gt; DHCP Table</b> screen ( <a href="#">Section 4.4 on page 44</a> ). Use this screen to view current DHCP client information.
Packet Statistics	Click <b>Details...</b> to go to the <b>Monitor &gt; Packet Statistics</b> screen ( <a href="#">Section 4.5 on page 45</a> ). Use this screen to view port status and packet specific statistics.

## 9.5 Wireless LAN General Screen

Use this screen to configure the wireless LAN settings of your NBG-419N. Go to **Configuration > Wireless LAN > General** to open the following screen.

**Figure 52** WISP Mode: LAN > General Screen



The following table describes the labels in this screen.

**Table 30** WISP Mode: LAN > General Screen

LABEL	DESCRIPTION
Wireless Setup	
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select the security mode of the access point to which you want to connect.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

### 9.5.0.1 No Security

Use this screen if the access point to which you want to connect does not use encryption.

**Figure 53** No Security (WISP)



The following table describes the labels in this screen.

**Table 31** No Security (WISP)

LABEL	DESCRIPTION
Wireless Setup	
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select <b>No Security</b> in this field.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 9.5.1 Static WEP

Use this screen if the access point to which you want to connect to uses WEP security mode.

**Figure 54** WEP (WISP)

The following table describes the labels in this screen..

**Table 32** WEP (WISP)

LABEL	DESCRIPTION
Wireless Setup	
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	

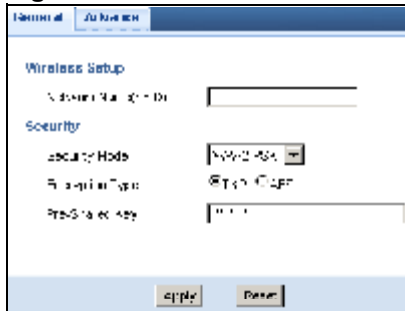
**Table 32** WEP (WISP)

LABEL	DESCRIPTION
Security Mode	Select <b>Static WEP</b> to enable data encryption.
PassPhrase	Enter a Passphrase (up to 26 printable characters) and click <b>Generate</b> .  A passphrase functions like a password. In WEP security mode, it is further converted by the NBG-419N into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network.
WEP Encryption	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> .  This dictates the length of the security key that the network is going to use.
Authentication Method	Select <b>Auto</b> or <b>Shared Key</b> from the drop-down list box.  This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at <b>Auto</b> unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs.  Select <b>Shared Key</b> to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key.  The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NBG-419N and the wireless stations must use the same WEP key for data transmission.  If you chose <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").  If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").  You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 9.5.2 WPA(2)-PSK

Use this screen if the access point to which you want to connect uses WPA(2)-PSK security mode.

**Figure 55** WPA-PSK/WPA2-PSK (WISP)



The following table describes the labels in this screen. .

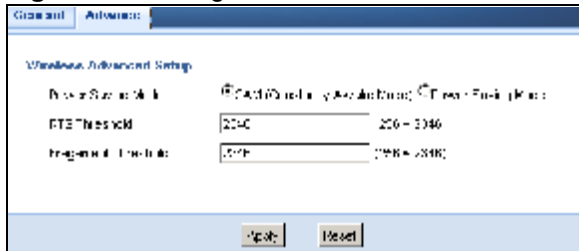
**Table 33** WPA-PSK/WPA2-PSK (WISP)

LABEL	DESCRIPTION
Wireless Setup	
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Encryption Type	Select the type of wireless encryption employed by the access point to which you want to connect.
Pre-Shared Key	<b>WPA-PSK/ WPA2-PSK</b> uses a simple common password for authentication. Type the pre-shared key employed by the access point to which you want to connect.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

### 9.5.3 Advance Screen

Use this screen to enable the power saving mode of your NBG-419N. Go to **Configuration > Wireless LAN** to open the following screen.

**Figure 56** Configuration > Wireless LAN > Advance Screen (WISP)



The following table describes the labels in this screen.

**Table 34** Configuration > Wireless LAN > Advance Screen (WISP)

LABEL	DESCRIPTION
Power Saving Mode	Select <b>CAM (Constantly Awake Mode)</b> if you do not want your NBG-419N to go to "sleep" when no wireless activity is detected in the Wireless LAN.  Select <b>Power Saving Mode</b> if you want the NBG-419N to go to sleep when no wireless connection is needed for a period of time. This means the NBG-419N consumes less electrical power.
RTS Threshold	This is the maximum data fragment size that can be sent in a wireless network before the AP fragments the packet into smaller data frames.
Fragment Threshold	This value controls how often wireless clients must get permission to send information to the AP. The lower the value, the more often the wireless clients must get permission. If this value is greater than the fragmentation threshold value, then wireless clients never have to get permission to send information to the AP.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.



## 10.1 Overview

This chapter provides tutorials for your NBG-419N as follows:

- [Connecting to the Internet from an Access Point](#)
- [Configuring Wireless Security Using WPS](#)
- [Enabling and Configuring Wireless Security \(No WPS\)](#)

## 10.2 Connecting to the Internet from an Access Point

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 access point wirelessly.

**Figure 57** Wireless Access Point Connection to the Internet



## 10.3 Configuring Wireless Security Using WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG-419N as the AP and NWD210N as the wireless client which connects to a notebook.

Note: 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 10.3.1 on page 90](#). 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 NBG-419N's interface. See [Section 10.3.2 on page 91](#). This is the more secure method, since one device can authenticate the other.

### 10.3.1 Push Button Configuration (PBC)

- 1 Make sure that your NBG-419N 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 NBG-419N's Web Configurator and press the **Push Button** button in the **Network > Wireless Client > WPS Station** screen.

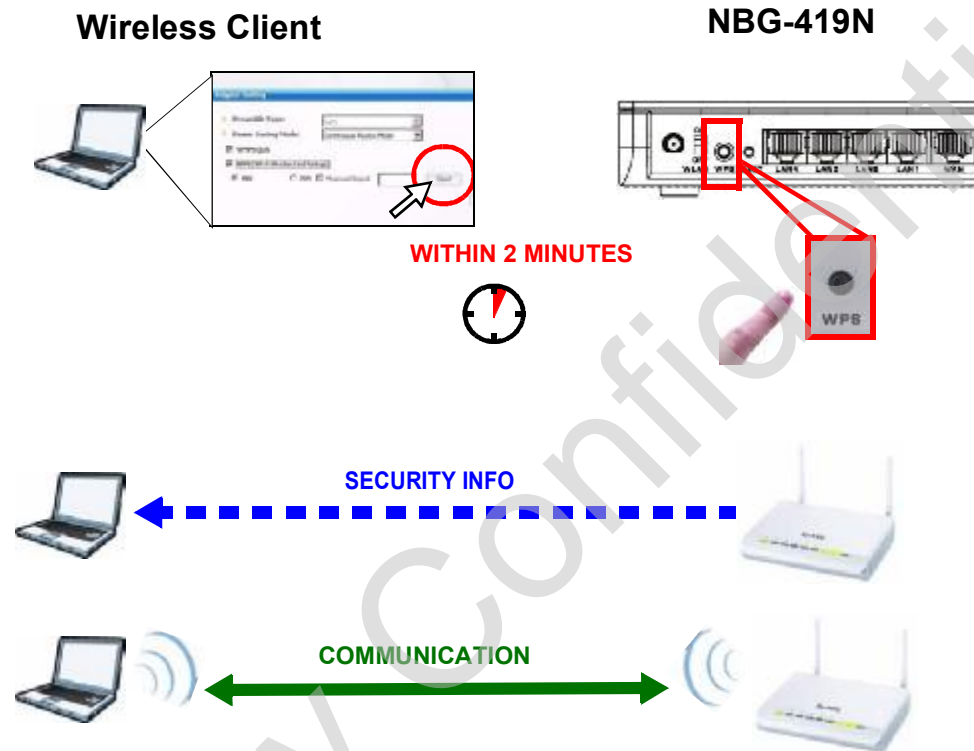
Note: Your NBG-419N has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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

The NBG-419N 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 NBG-419N securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG-419N and wireless client (the NWD210N in this example).

**Figure 58** Example WPS Process: PBC Method



### 10.3.2 PIN Configuration

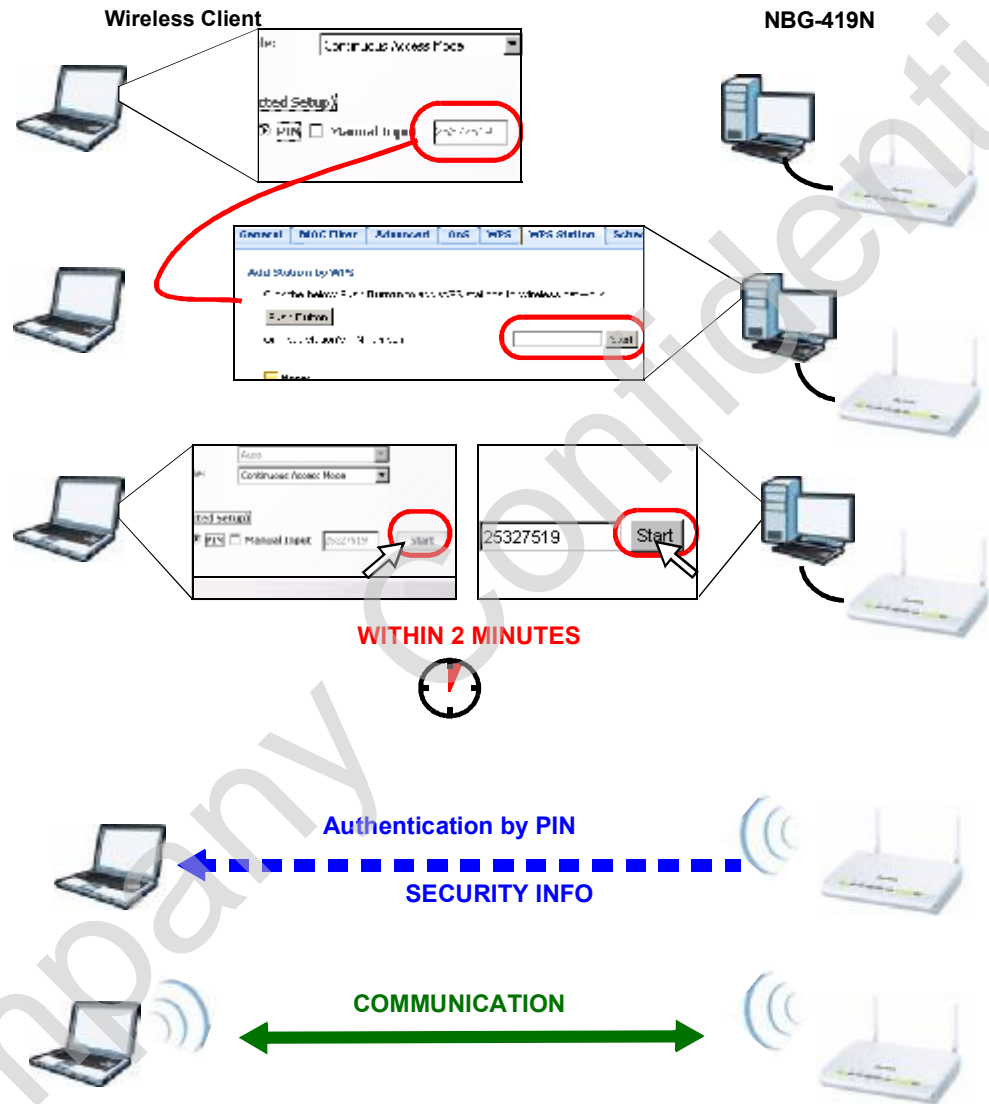
When you use the PIN configuration method, you need to use both NBG-419N's configuration interface and the client's utilities.

- 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 NBG-419N.
- 3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG-419N's **WPS Station** screen within two minutes.

The NBG-419N 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 NBG-419N securely.

The following figure shows you the example to set up wireless network and security on NBG-419N and wireless client (ex. NWD210N in this example) by using PIN method.

**Figure 59** Example WPS Process: PIN Method



## 10.4 Enabling and Configuring Wireless Security (No WPS)

This example shows you how to configure wireless security settings with the following parameters on your NBG-419N.

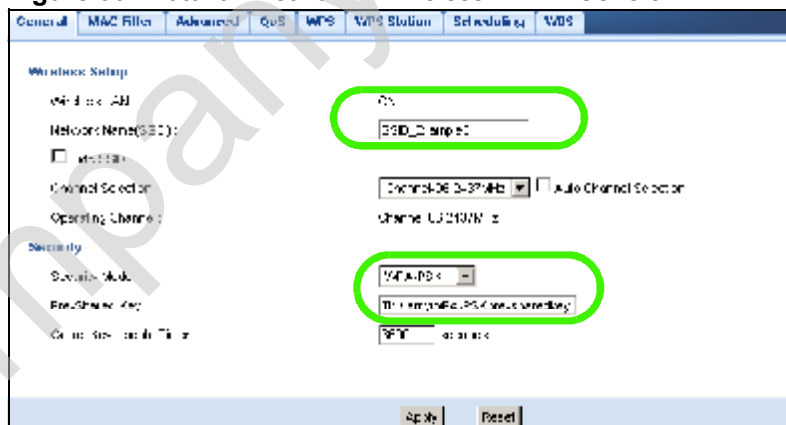
<b>SSID</b>	SSID_Example3
<b>Channel</b>	6
<b>Security</b>	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG-419N.

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](#)).

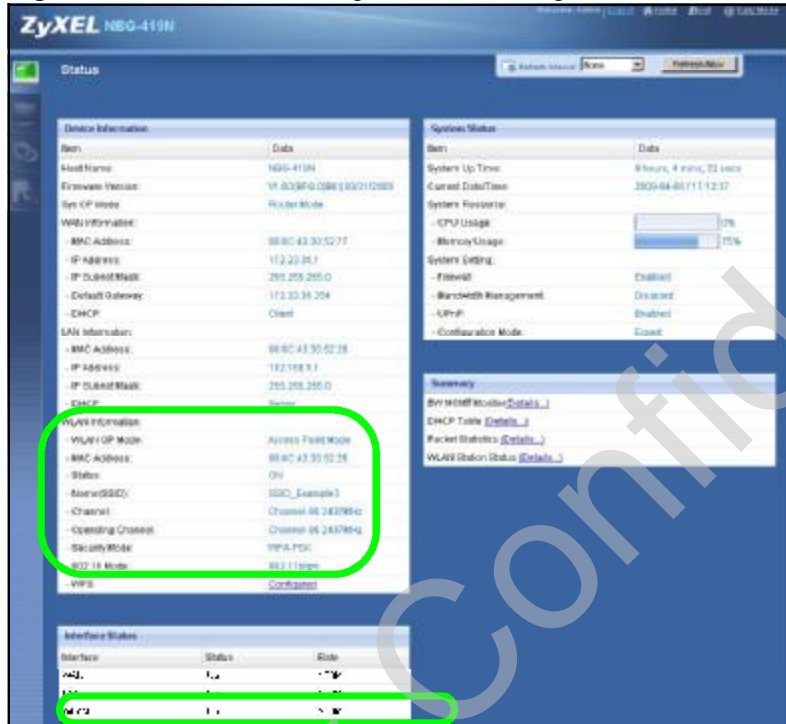
- 1 Open the **Wireless LAN > General** screen in the AP's Web Configurator.
- 2 Make sure the **Enable Wireless LAN** check box is selected.
- 3 Enter **SSID\_Example3** as the SSID and select a channel.
- 4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

**Figure 60** Tutorial: Network > Wireless LAN > General



- 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 61** Tutorial: Checking Wireless Settings



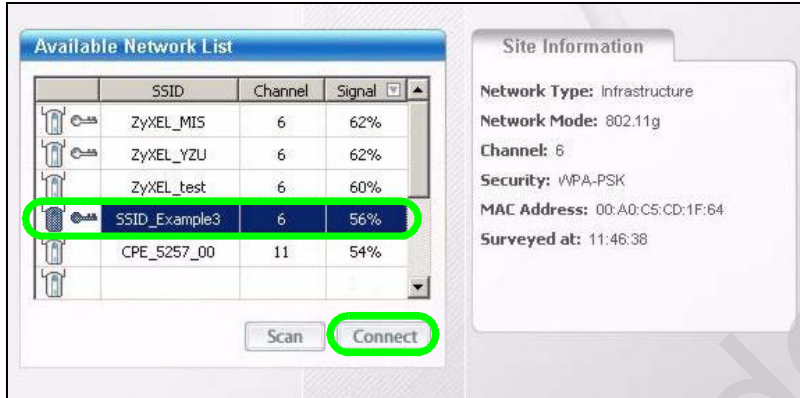
### 10.4.1 Configure Your Notebook

Note: 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 NBG-419N 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.

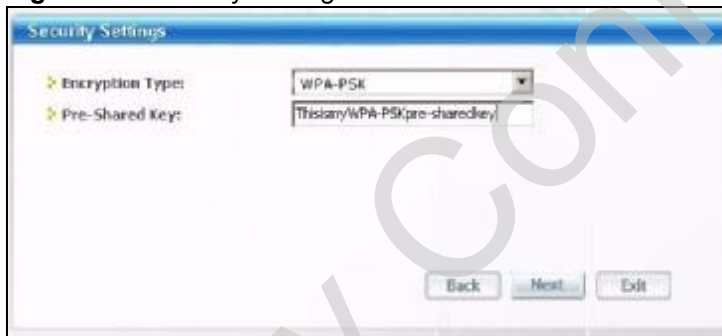
- 4 Select SSID\_Example3 and click **Connect**.

**Figure 62** Connecting a Wireless Client to a Wireless Network t



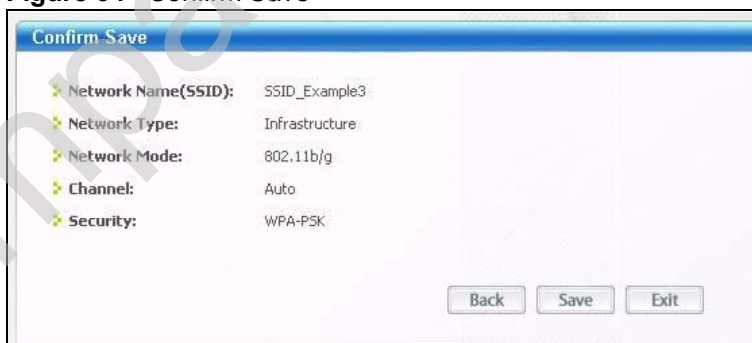
- 5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

**Figure 63** Security Settings



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

**Figure 64** 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 65** Link Status



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.



---

# PART II

## Network

---

Wireless LAN (99)

WAN (119)

LAN (135)

DHCP Server (139)

Network Address Translation (NAT) (143)

Dynamic DNS (151)

Static Route (153)

RIP (157)

Company Confidential

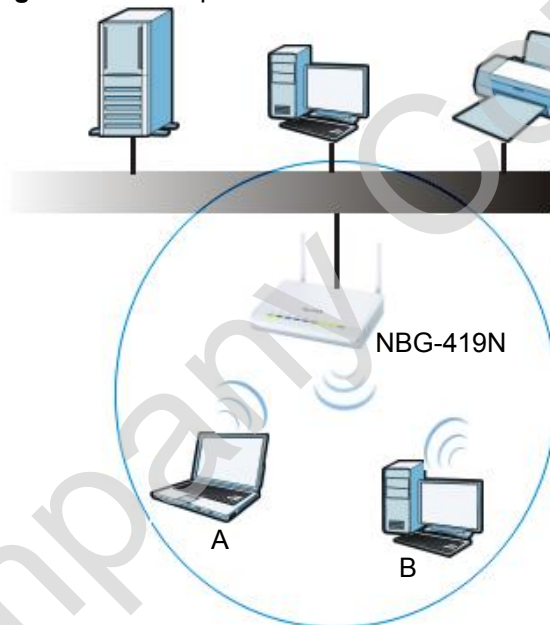
# Wireless LAN

## 11.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG-419N. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

**Figure 66** 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 NBG-419N is the AP.

## 11.2 What You Can Do

- Use the **General** screen ([Section 11.4 on page 103](#)) to enable the Wireless LAN, enter the SSID and select the wireless security mode.
- Use the **MAC Filter** screen ([Section 11.5 on page 109](#)) to allow or deny wireless stations based on their MAC addresses from connecting to the NBG-419N.
- Use the **Advanced** screen ([Section 11.6 on page 110](#)) to allow wireless advanced features, such as intra-BSS networking and set the RTS/CTS Threshold.
- Use the **QoS** screen ([Section 11.7 on page 111](#)) to set priority levels to services, such as e-mail, VoIP, chat, and so on.
- Use the **WPS** screen ([Section 11.8 on page 112](#)) to quickly set up a wireless network with strong security, without having to configure security settings manually.
- Use the **WPS Station** screen ([Section 11.9 on page 113](#)) to add a wireless station using WPS.
- Use the **Scheduling** screen ([Section 11.10 on page 114](#)) to set the times your wireless LAN is turned on and off.
- Use the **WDS** screen ([Section 11.11 on page 115](#)) to configure Wireless Distribution System on your NBG-419N.

## 11.3 What You Should Know

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.

### 11.3.1 Wireless Security Overview

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

### 11.3.1.1 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.

### 11.3.1.2 MAC Address Filter

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

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

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

### 11.3.1.3 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.

- 
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.

The types of encryption you can choose depend on the type of user authentication.

**Table 35** Types of Encryption for Each Type of Authentication

	<b>NO AUTHENTICATION</b>
<b>Weakest</b>	No Security
↕	WEP
	WPA-PSK
	<b>WPA2-PSK</b>
<b>Strongest</b>	

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA-PSK. Therefore, you should set up **WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK** 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.

When you select **WPA2-PSK** in your NBG-419N, 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** (depending on the type of wireless network login) and select the **WPA Compatible** option in the NBG-419N.

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.

#### 11.3.1.4 WPS

WiFi Protected Setup (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. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the [Section 10.3 on page 89](#).

#### 11.3.1.5 WDS

Wireless Distribution System or WDS security is used between bridged APs. It is independent of the security between the wired networks and their respective APs. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key.

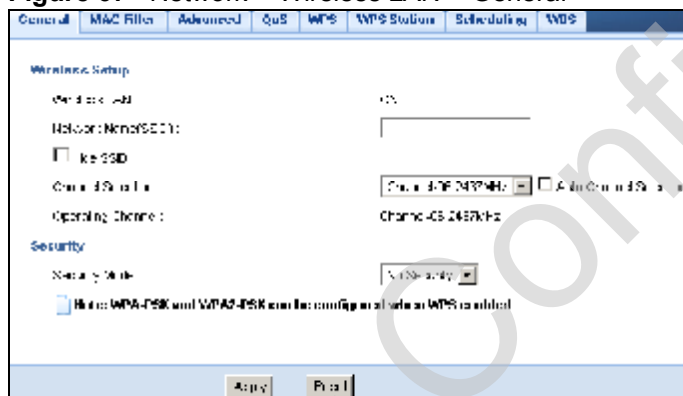
## 11.4 General Wireless LAN Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the NBG-419N from a computer connected to the wireless LAN and you change the NBG-419N'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 NBG-419N's new settings.

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

**Figure 67** Network > Wireless LAN > General



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

**Table 36** Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN	This is turned on by default. You can turn the wireless LAN on or off using the switch at the rear panel of the NBG-419N. The current wireless state is reflected in this field.
Network Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the NBG-419N must have the same SSID. Enter a descriptive name (up to 32 keyboard 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 <b>Auto Channel Selection</b> is disabled.

**Table 36** Network > Wireless LAN > General

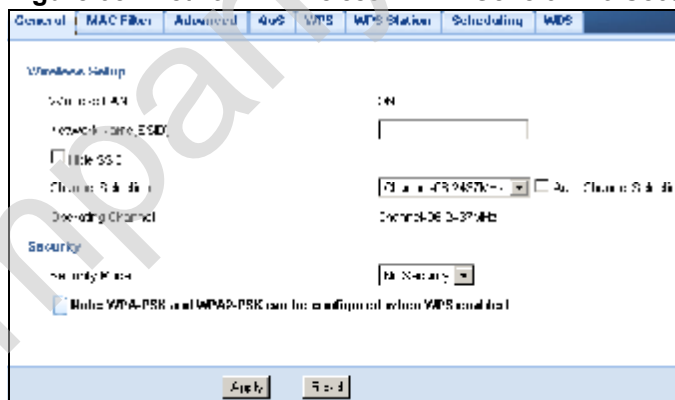
LABEL	DESCRIPTION
Operating Channel	This displays the channel the NBG-419N is currently using.
Security	
Security Mode	Select <b>WEP</b> , <b>WPA-PSK</b> or <b>WPA2-PSK</b> to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the NBG-419N. After you select to use a security, additional options appears in this screen. See <a href="#">11.4.2</a> and <a href="#">11.4.3</a> sections.  Or you can select <b>No Security</b> to allow any client to associate this network without authentication.  Note: If you enable the WPS function, only <b>No Security</b> , <b>WPA-PSK</b> and <b>WPA2-PSK</b> are available in this field.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

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

### 11.4.1 No Security

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

Note: If you do not enable any wireless security on your NBG-419N, your network is accessible to any wireless networking device that is within range.

**Figure 68** Network > Wireless LAN > General: No Security



The following table describes the labels in this screen.

**Table 37** Network > Wireless LAN > General: No Security

LABEL	DESCRIPTION
Security Mode	Choose <b>No Security</b> from the drop-down list box.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

Refer to [Table 36 on page 103](#) for descriptions of the other labels in this screen.

## 11.4.2 WEP Encryption

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

Your NBG-419N 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 69** Network > Wireless LAN > General: Static WEP

The screenshot shows the 'General' tab of the wireless LAN configuration page. Under 'Wireless Setup', 'Wireless LAN' is turned ON, the SSID is 'NBG-419N', and the channel is set to 'Channel-06 2437MHz'. Under the 'Security' section, 'Security Mode' is set to 'Static WEP', 'WEP Encryption' is set to '64-bits', and 'Authentication Method' is 'Shared Key'. There are four key input fields labeled 'Key 1' through 'Key 4', with 'Hex' selected as the input format. A 'Generate' button is next to the passphrase field. 'Apply' and 'Reset' buttons are at the bottom.

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

**Table 38** Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Security Mode	Select <b>Static WEP</b> to enable data encryption.
PassPhrase	Enter a Passphrase (up to 26 printable characters) and click Generate. A passphrase functions like a password. In WEP security mode, it is further converted by the NBG-419N into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network.
WEP Encryption	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> . This dictates the length of the security key that the network is going to use.

**Table 38** Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Authentication Method	<p>Select <b>Auto</b> or <b>Shared Key</b> from the drop-down list box.</p> <p>This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at <b>Auto</b> unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs.</p> <p>Select <b>Shared Key</b> to force the clients to provide the WEP key prior to communication.</p>
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	<p>Select this option in order to enter hexadecimal characters as a WEP key.</p> <p>The preceding "0x", that identifies a hexadecimal key, is entered automatically.</p>
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the NBG-419N and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose <b>64-bit WEP</b>, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose <b>128-bit WEP</b>, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure at least one key, only one key can be activated at any one time. The default key is key 1.</p>
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

Refer to [Table 36 on page 103](#) for descriptions of the other labels in this screen.

### 11.4.3 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 70** Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

**Table 39** Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Select <b>WPA-PSK</b> or <b>WPA2-PSK</b> to enable data encryption.
WPA-PSK Compatible	This field appears when you choose <b>WPA-PSK2</b> as the <b>Security Mode</b> . Check this field to allow wireless devices using <b>WPA-PSK</b> security mode to connect to your NBG-419N.
Pre-Shared Key	<b>WPA-PSK/WPA2-PSK</b> uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the AP sends a new group key out to all clients. The default is <b>3600</b> seconds (60 minutes).
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

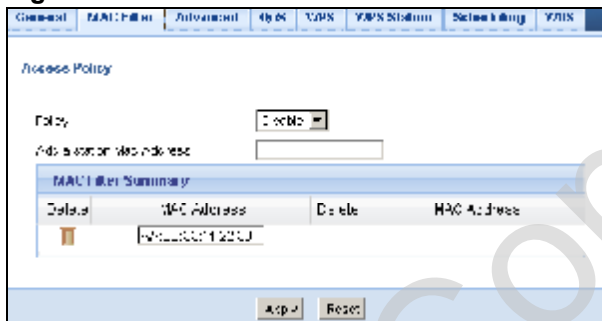
Refer to [Table 36 on page 103](#) for descriptions of the other labels in this screen.

## 11.5 MAC Filter

The MAC filter screen allows you to configure the NBG-419N to give exclusive access to devices (Allow) or exclude devices from accessing the NBG-419N (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your NBG-419N's MAC filter settings, click **Network > Wireless LAN > MAC Filter**. The screen appears as shown.

**Figure 71** Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

**Table 40** Network > Wireless LAN > MAC Filter

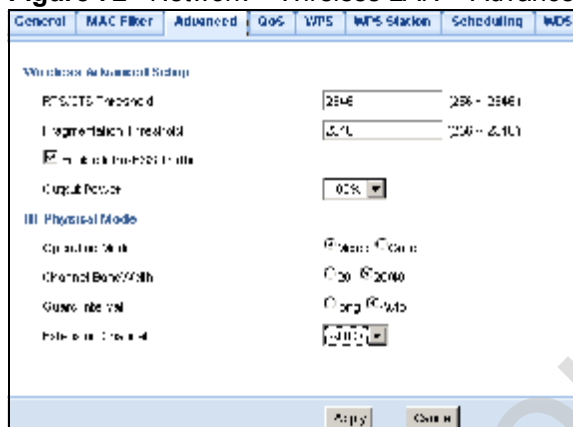
LABEL	DESCRIPTION
Access Policy	
Policy	Define the filter action for the list of MAC addresses in the <b>MAC Address</b> table.  Select <b>Allow</b> to permit access to the NBG-419N, MAC addresses not listed will be denied access to the NBG-419N.  Select <b>Reject</b> to block access to the NBG-419N, MAC addresses not listed will be allowed to access the NBG-419N
Add a station Mac Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the NBG-419N in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. Click <b>Add</b> .
MAC Filter Summary	
Delete	Click the delete icon to remove the MAC address from the list.
MAC Address	This is the MAC address of the wireless station that are allowed or denied access to the NBG-419N.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 11.6 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as intra-BSS networking and set the RTS/CTS Threshold

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

**Figure 72** Network > Wireless LAN > Advanced



The following table describes the labels in this screen.

**Table 41** Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 256 and 2432.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between <b>256</b> and <b>2346</b> .
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client <b>A</b> and <b>B</b> can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client <b>A</b> and <b>B</b> can still access the wired network but cannot communicate with each other.
Output Power	Set the output power of the NBG-419N in this field. If there is a high density of APs in an area, decrease the output power of the NBG-419N to reduce interference with other APs. Select one of the following <b>100%</b> , <b>90%</b> , <b>75%</b> , <b>50%</b> , <b>25%</b> , <b>10%</b> or <b>Minimum</b> . See the product specifications for more information on your NBG-419N's output power.
HT (High Throughput) Physical Mode - Use the fields below to configure the 802.11 wireless environment of your NBG-419N.	

**Table 41** Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Operating Mode	Choose this according to the wireless mode(s) used in your network.  <b>Mixed Mode</b> - Select this if the wireless clients in your network use different wireless modes (for example, IEEE 802.11b/g and IEEE 802.11n modes)  <b>Green Mode</b> - Select this if the wireless clients in your network uses only one type of wireless mode (for example, IEEE 802.11n only)
Channel Bandwidth	Select the channel bandwidth you want to use for your wireless network. It is recommended that you select <b>20/40</b> (20/40 MHz).  Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood.
Guard Interval	Select <b>Auto</b> to increase data throughput. However, this may make data transfer more prone to errors.  Select <b>Long</b> to prioritize data integrity. This may be because your wireless network is busy and congested or the NBG-419N is located in an environment prone to radio interference.
Extension Channel	This is set to <b>Auto</b> by default.  If you select <b>20/40</b> as your <b>Channel Bandwidth</b> , the extension channel enables the NBG-419N to get higher data throughput. This also lowers radio interference and traffic.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 11.7 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as VoIP and video) a priority level.

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

**Figure 73** Network > Wireless LAN > QoS

The screenshot shows the 'QoS' configuration page. At the top, there are tabs for 'General', 'MAC Filter', 'Advanced', 'QoS', 'WPS', 'WPS Station', 'Scheduling', and 'WDS'. The 'QoS' tab is active. Below the tabs, the 'WMM Configuration' section is visible, containing a checkbox labeled 'Enable WMM QoS' which is checked. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

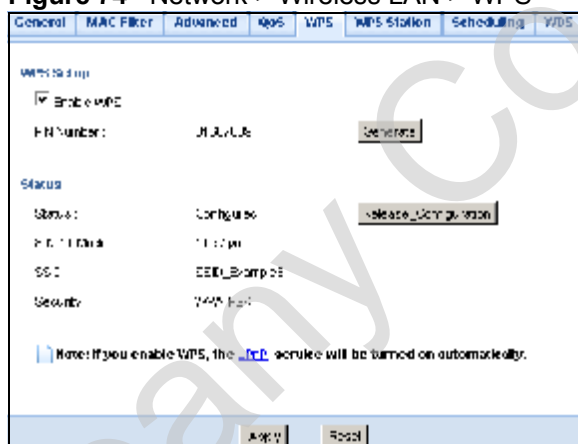
**Table 42** Network > Wireless LAN > QoS

LABEL	DESCRIPTION
Enable WMM QoS	Check this to have the NBG-419N automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Apply	Click <b>Apply</b> to save your changes to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 11.8 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network > Wireless LAN > WPS** tab.

**Figure 74** Network > Wireless LAN > WPS



The following table describes the labels in this screen.

**Table 43** Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click <b>Generate</b> to generate a new PIN number.
Status	



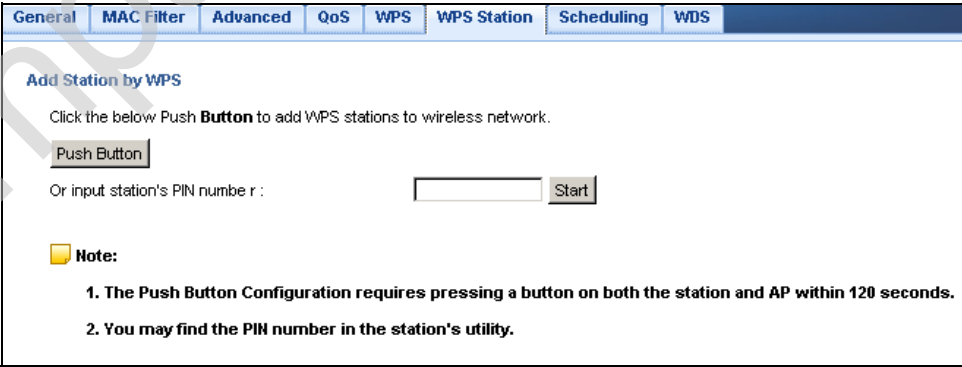
**Table 43** Network > Wireless LAN > WPS

LABEL	DESCRIPTION
Status	This displays <b>Configured</b> when the NBG-419N has connected to a wireless network using WPS or when <b>Enable WPS</b> is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen.  This displays <b>Unconfigured</b> if WPS is disabled and there are no wireless or wireless security changes on the NBG-419N or you click <b>Release_Configuration</b> to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays <b>Configured</b> .  Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG-419N.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the NBG-419N.
SSID	This is the name of the wireless network.
Security	This is the type of wireless security employed by the network.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Refresh	Click <b>Refresh</b> to get this screen information afresh.

## 11.9 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network > Wireless LAN > WPS Station** tab.

Note: Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

**Figure 75** Network > Wireless LAN > WPS Station


**Add Station by WPS**

Click the below **Push Button** to add WPS stations to wireless network.

Or input station's PIN number r :

**Note:**

1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.

The following table describes the labels in this screen.

**Table 44** Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See <a href="#">Section 10.3.1 on page 90</a> .  Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See <a href="#">Section 10.3.2 on page 91</a> .  Type the same PIN number generated in the wireless station's utility. Then click <b>Start</b> to associate to each other and perform the wireless security information synchronization.

## 11.10 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network > Wireless LAN > Scheduling** tab.

**Figure 76** Network > Wireless LAN > Scheduling

**Wireless LAN Scheduling**

Enable Wireless LAN Scheduling

WLAN status	Day	For the following times (24-Hour Format)			
<input type="radio"/> On <input checked="" type="radio"/> Off	<input checked="" type="checkbox"/> Everyday	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Mon	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Tue	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Wed	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Thu	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Fri	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Sat	00 (hour)	00 (min)	~	00 (hour) 00 (min)
<input type="radio"/> On <input checked="" type="radio"/> Off	<input type="checkbox"/> Sun	00 (hour)	00 (min)	~	00 (hour) 00 (min)

**Note:** Specify the same begin time and end time means the whole day schedule.

Apply Reset

The following table describes the labels in this screen.

**Table 45** Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Scheduling	
WLAN Status	Select <b>On</b> or <b>Off</b> to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the <b>Day</b> and <b>Except for the following times</b> fields.
Day	Select <b>Everyday</b> or the specific days to turn the Wireless LAN on or off. If you select <b>Everyday</b> you can not select any specific days. This field works in conjunction with the <b>Except for the following times</b> field.
For the following times (24-Hour Format)	Select a begin time using the first set of <b>hour</b> and minute ( <b>min</b> ) drop down boxes and select an end time using the second set of <b>hour</b> and minute ( <b>min</b> ) drop down boxes. If you have chosen <b>On</b> earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen <b>Off</b> earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 11.11 WDS Screen

A Wireless Distribution System is a wireless connection between two or more APs. Use this screen to set the operating mode of your NBG-419N to **AP + Bridge** or **Bridge Only** and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

Note: You must enable the same wireless security settings on the NBG-419N and on all wireless clients that you want to associate with it.

Click **Network > Wireless LAN > WDS** tab. The following screen opens with the **Basic Setting** set to **Disabled**, and **Security Mode** set to **No Security**.

**Figure 77** Network > Wireless LAN > WDS

The screenshot shows the WDS Setup configuration page. It features a navigation bar with tabs: General, MAC Filter, Advanced, QoS, WPS, WPS Station, Scheduling, and WDS. The main content area is titled 'WDS Setup' and is divided into two sections: 'Basic Setting' and 'Security'. In the 'Basic Setting' section, there is a dropdown menu for 'Basic Setting' set to 'AP+Bridge', a text field for 'Local MAC Address' containing '00:0C:43:30:52:28', a dropdown menu for 'Phy Mode' set to 'CCK', and four empty text fields for 'Remote MAC Address'. In the 'Security' section, there is a dropdown menu for 'EncrypType' set to 'WEP' and an empty text field for 'Encryp Key'. At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 46** Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS Setup	
Basic Settings	Select the operating mode for your NBG-419N. <ul style="list-style-type: none"> <li><b>AP + Bridge</b> - The NBG-419N functions as a bridge and access point simultaneously.</li> <li><b>Bridge</b> - The NBG-419N acts as a wireless network bridge and establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The NBG-419N can establish up to five wireless links with other APs.</li> </ul>
Local MAC Address	This is the MAC address of your NBG-419N.
Phy Mode	Select the Phy mode you want the NBG-419N to use. This dictates the maximum size of packets during data transmission.
Remote MAC Address	This is the MAC address of the peer device that your NBG-419N wants to make a bridge connection with.  You can connect to up to 4 peer devices.
Security	
EncrypType	Select whether to use <b>WEP</b> , <b>TKIP</b> or <b>AES</b> encryption for your WDS connection in this field.  Otherwise, select <b>No Security</b> .
EncrypKey	The Encryp key is used to encrypt data. Peers must use the same key for data transmission.

**Table 46** Network > Wireless LAN > WDS

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes to NBG-419N.
Refresh	Click <b>Refresh</b> to reload the previous configuration for this screen.

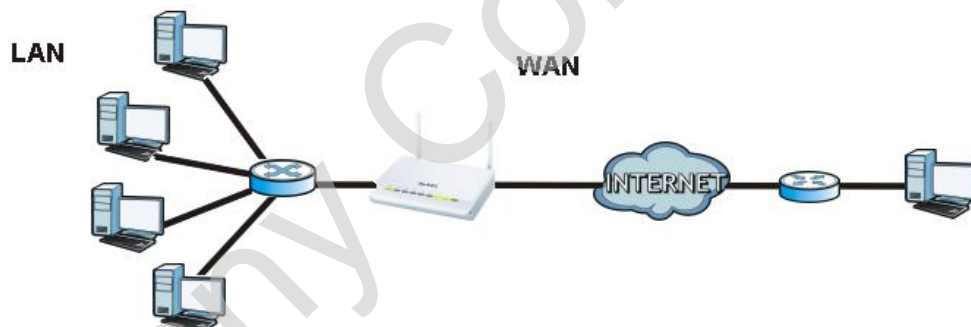
Company Confidential

## 12.1 Overview

This chapter discusses the NBG-419N's **WAN** screens. Use these screens to configure your NBG-419N for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

**Figure 78** LAN and WAN



## 12.2 What You Can Do

- Use the **Internet Connection** screen ([Section 12.4 on page 122](#)) to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses.
- Use the **Advanced** screen ([Section 12.5 on page 132](#)) to enable multicasting, configure Windows networking and bridge.
- Use **IGMP Snooping** screen ([Section 12.6 on page 132](#)) to enable IGMP snooping in the LAN ports.

## 12.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your NBG-419N.

### 12.3.1 Configuring Your Internet Connection

#### Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPTP (Point-to-Point Tunneling Protocol), they should also provide a username and password (and service name) for user authentication.

#### WAN IP Address

The WAN IP address is an IP address for the NBG-419N, which makes it accessible from an outside network. It is used by the NBG-419N to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG-419N tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

#### DNS Server Address Assignment

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

The NBG-419N can get the DNS server addresses in the following ways.

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the NBG-419N's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.



### WAN MAC Address

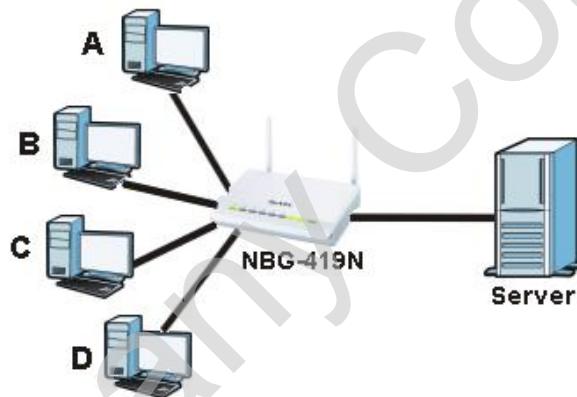
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

### 12.3.2 Multicast

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

**Figure 79** Multicast Example



In the multicast example above, systems A and D comprise one multicast group. In multicasting, the server only needs to send one data stream and this is delivered to systems A and D.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. The NBG-419N supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the NBG-419N queries all directly connected networks to gather group membership. After that, the NBG-419N periodically updates this information. IP multicasting can be enabled/disabled on the NBG-419N LAN and/or WAN

interfaces in the Web Configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

## 12.4 Internet Connection

Use this screen to change your NBG-419N's Internet access settings. Click **WAN** from the Configuration menu. The screen differs according to the encapsulation you choose.

### 12.4.1 Ethernet Encapsulation

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

**Figure 80** Network > WAN > Internet Connection: Ethernet Encapsulation

The screenshot shows the 'Internet Connection' configuration page for Ethernet encapsulation. The page has three tabs: 'Internet Connection', 'Advanced', and 'IGMP Snooping'. The 'Internet Connection' tab is active. The page is divided into several sections:

- ISP Parameters for Internet Access:** Encapsulation is set to 'Ethernet'.
- WAN IP Address Assignment:** The 'Get automatically from ISP (Default)' radio button is selected. Below it, the 'Use Fixed IP Address' radio button is unselected. The IP Address is 172.1.1.1, IP Subnet Mask is 255.255.255.0, and Gateway IP Address is 172.1.1.254.
- WAN DNS Assignment:** The First DNS Server is set to 'From ISP' with a value of 0.0.0.0. The Second DNS Server is also set to 'From ISP' with a value of 0.0.0.0.
- WAN MAC Address:** The 'Factory default' radio button is selected. The 'Clone the computer's MAC address - IP Address' radio button is unselected with a value of 192.168.1.33. The 'Set WAN MAC Address' radio button is unselected with a value of 00:00:00:00:00:00.

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

The following table describes the labels in this screen.

**Table 47** Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet.
WAN IP Address Assignment	
Get automatically from ISP (Default)	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
IP Subnet Mask	Enter the <b>IP Subnet Mask</b> in this field.
Gateway IP Address	Enter a <b>Gateway IP Address</b> (if your ISP gave you one) in this field.
WAN DNS Assignment	
First DNS Server Second DNS Server	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the NBG-419N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG-419N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select <b>Factory default</b> to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select <b>Clone the computer's MAC address - IP Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 12.4.2 PPPoE Encapsulation

The NBG-419N supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

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

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

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

By implementing PPPoE directly on the NBG-419N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG-419N does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

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

**Figure 81** Network > WAN > Internet Connection: PPPoE Encapsulation

The screenshot shows the configuration page for PPPoE encapsulation. It includes the following fields and options:

- ISP Parameters for Internet Access:** Encapsulation (PPP over Ethernet), User Name (pppoe\_user), Password (masked), Retype to Confirm (masked), MTU Size (1454), Nailed-Up Connection (checked), Idle Timeout (100 seconds).
- WAN IP Address Assignment:** Get automatically from ISP (selected), Use Fixed IP Address (unselected), My WAN IP Address (0.0.0.0).
- WAN DNS Assignment:** First DNS Server (From ISP, 0.0.0.0), Second DNS Server (From ISP, 0.0.0.0).
- WAN MAC Address:** Factory default (selected), Clone the computer's MAC address - IP Address (192.168.1.33), Set WAN MAC Address (00:00:00:00:00:00).

Buttons for 'Apply' and 'Reset' are located at the bottom of the form.

The following table describes the labels in this screen.

**Table 48** Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select <b>PPP over Ethernet</b> if you connect to your Internet via dial-up.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your NBG-419N can receive and process.
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.

**Table 48** Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
Idle Timeout (sec)	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
WAN DNS Assignment	
First DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the NBG-419N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
Second DNS Server	Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> .  Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the NBG-419N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select <b>Factory default</b> to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select <b>Clone the computer's MAC address - IP Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 12.4.3 PPTP Encapsulation

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

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

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

**Figure 82** Network > WAN > Internet Connection: PPTP Encapsulation

The screenshot shows the configuration page for PPTP Encapsulation. The page is titled "Internet Connection" and has tabs for "Advanced" and "IGMP Snooping". The configuration is organized into several sections:

- ISP Parameters for Internet Access:**
  - Encapsulation: PPTP (dropdown)
  - User Name: pptp\_user
  - Password: [Redacted]
  - Retype to Confirm: [Redacted]
  - Nailed-Up Connection
  - Idle Timeout (sec): 100 (in seconds)
- PPTP Configuration:**
  - Server IP Address: 172.1.1.254
  - Get automatically from ISP
  - Use Fixed IP Address
  - IP Address: 172.1.1.1
  - IP Subnet Mask: 255.255.255.0
  - Gateway IP Address: 172.1.1.254
- WAN IP Address Assignment:**
  - Get automatically from ISP
  - Use Fixed IP Address
  - My WAN IP Address: 0.0.0.0
- WAN DNS Assignment:**
  - First DNS Server: From ISP (dropdown), 9.0.0.0
  - Second DNS Server: From ISP (dropdown), 9.0.0.0
- WAN MAC Address:**
  - Factory default
  - Clone the computer's MAC address - IP Address: 192.168.1.33
  - Set WAN MAC Address: 00:00:00:00:00:00

At the bottom of the page, there are "Apply" and "Reset" buttons.

The following table describes the labels in this screen.

**Table 49** Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Nailed-up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the NBG-419N automatically disconnects from the PPTP server.
PPTP Configuration	
Server IP Address	Type the IP address of the PPTP server.
Get automatically from ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
IP Subnet Mask	Your NBG-419N 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 NBG-419N.
Gateway IP Address	Enter a <b>Gateway IP Address</b> (if your ISP gave you one) in this field.
WAN IP Address Assignment	
Get automatically from ISP	Select this to get your WAN IP address from your ISP.
Use Fixed IP Address	Select this option if the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
WAN DNS Assignment	



**Table 49** Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
First DNS Server Second DNS Server	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the NBG-419N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG-419N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select <b>Factory default</b> to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select <b>Clone the computer's MAC address - IP Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

#### 12.4.4 L2TP Encapsulation

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peer devices over another network (like the Internet).

This screen displays when you select **L2TP** encapsulation.

**Figure 83** Network > WAN > Internet Connection: L2TP Encapsulation

The following table describes the labels in this screen.

**Table 50** Network > WAN > Internet Connection: L2TP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	To configure a L2TP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a layer-2 connection and the L2TP parameters for an L2TP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
L2TP Configuration	
Server IP Address	Type the IP address of the L2TP server.
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.

**Table 50** Network > WAN > Internet Connection: L2TP Encapsulation

LABEL	DESCRIPTION
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
IP Subnet Mask	Your NBG-419N 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 NBG-419N.
Gateway IP Address	Enter a <b>Gateway IP Address</b> (if your ISP gave you one) in this field.
WAN IP Address Assignment	
Get automatically from ISP	Select this to get your WAN IP address from your ISP.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
WAN DNS Assignment	
First DNS Server Second DNS Server	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the NBG-419N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG-419N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select <b>Factory default</b> to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select <b>Clone the computer's MAC address - IP Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 12.5 Advanced WAN Screen

Use this screen to enable **Multicast** and enable **Auto-bridge**.

Note: The categories shown in this screen are independent of each other.

To change your NBG-419N's advanced WAN settings, click **Network > WAN > Advanced**. The screen appears as shown.

**Figure 84** Network > WAN > Advanced

The following table describes the labels in this screen.

**Table 51** Network > WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Select <b>IGMPv1/v2</b> to enable multicasting. This applies to traffic routed from the WAN to the LAN. Select <b>None</b> to disable this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.
Auto-bridge	
Enable Auto-bridge mode	Select this option to have the NBG-419N switch to bridge mode automatically when the NBG-419N gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) no matter what the LAN IP address is.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 12.6 IGMP Snooping Screen

Use this screen to enable IGMP snooping if you have LAN users that subscribe to multicast services.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data.

Click **Network > WAN > IGMP Snooping**. The screen appears as shown.

**Figure 85** Network > WAN > IGMP Snooping

The following table describes the labels in this screen.

**Table 52** Network > WAN > IGMP Snooping

LABEL	DESCRIPTION
Auto-bridge	
Enable IGMP Snooping	Select this option to have the NBG-419N use IGMP snooping. Check the LAN port/s to which IGMP snooping applies.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

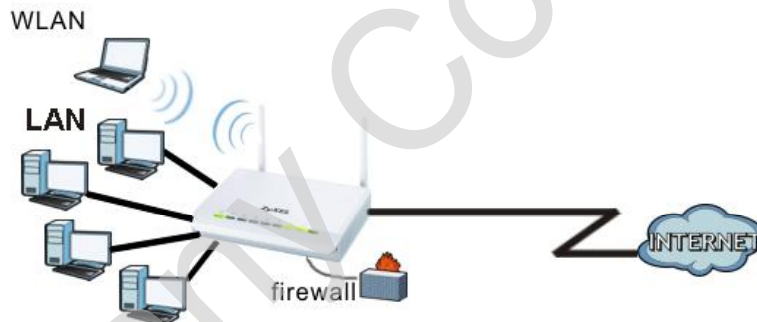
Company Confidential

## 13.1 Overview

This chapter describes how to configure LAN settings.

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

**Figure 86** LAN Example



The LAN screens can help you manage IP addresses.

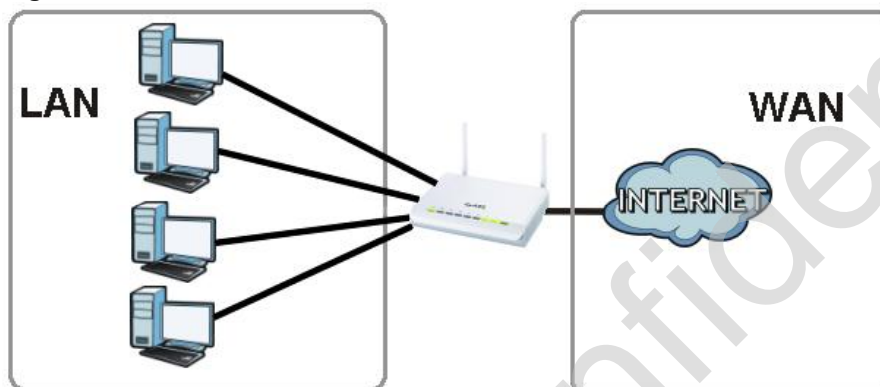
## 13.2 What You Can Do

- Use the **IP** screen ([Section 13.4 on page 137](#)) to change the IP address for your NBG-419N.
- Use the **IP Alias** screen ([Section 13.5 on page 138](#)) to have the NBG-419N apply IP alias to create LAN subnets.

## 13.3 What You Need To Know

The actual physical connection determines whether the NBG-419N ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

**Figure 87** LAN and WAN IP Addresses



The LAN parameters of the NBG-419N are preset in the factory with the following values:

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

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

### 13.3.1 IP Pool Setup

The NBG-419N is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the NBG-419N itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

### 13.3.2 LAN TCP/IP

The NBG-419N has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.



### 13.3.3 IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The NBG-419N supports three logical LAN interfaces via its single physical Ethernet interface with the NBG-419N itself as the gateway for each LAN network.

## 13.4 LAN IP Screen

Use this screen to change the IP address for your NBG-419N. Click **Network > LAN > IP**.

**Figure 88** Network > LAN > IP

The following table describes the labels in this screen.

**Table 53** Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your NBG-419N in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG-419N 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 NBG-419N.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 13.5 IP Alias Screen

Use this screen to have the NBG-419N apply IP alias to create LAN subnets. Click **LAN > IP Alias**.

**Figure 89** Network > LAN > IP Alias

The following table describes the labels in this screen.

**Table 54** Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias	Check this to enable IP alias.
IP Address	Type the IP alias address of your NBG-419N in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG-419N 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 NBG-419N.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# DHCP Server

## 14.1 Overview

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 NBG-419N's LAN as a DHCP server or disable it. When configured as a server, the NBG-419N provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

## 14.2 What You Can Do

- Use the **General** ([Section 14.3 on page 139](#)) screen to enable the DHCP server.
- Use the **Advanced** ([Section 14.4 on page 140](#)) screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

## 14.3 General Screen

Use this screen to enable the DHCP server. Click **Network > DHCP Server**. The following screen displays.

**Figure 90** Network > DHCP Server > General

General	Advanced
<b>LAN DHCP Setup</b>	
<input checked="" type="checkbox"/> Enable DHCP Server	
IP Pool Starting Address	Pool Size
192.168.1.33	32
Apply    Reset	

The following table describes the labels in this screen.

**Table 55** Network > DHCP Server > General

LABEL	DESCRIPTION
Enable DHCP Server	Enable or Disable DHCP for LAN.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 14.4 Advanced Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the NBG-419N sends to the DHCP clients.

To change your NBG-419N's static DHCP settings, click **Network > DHCP Server > Advanced**. The following screen displays.

**Figure 91** Network > DHCP Server > Advanced

The screenshot shows the 'Advanced' configuration screen for the DHCP Server. It features a 'LAN Static DHCP Table' with 8 rows, each containing a MAC address and an IP address. Below the table, there is a 'DNS Server' section with two rows for 'First DNS Server' and 'Second DNS Server', each with a dropdown menu and a text input field. The 'Apply' and 'Reset' buttons are located at the bottom of the screen.

The following table describes the labels in this screen.

**Table 56** Network > DHCP Server > Advanced

LABEL	DESCRIPTION
LAN Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
DNS Server	
DNS Servers Assigned by DHCP Server	The NBG-419N passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG-419N only passes this information to the LAN DHCP clients when you select the <b>Enable DHCP Server</b> check box. When you clear the <b>Enable DHCP Server</b> check box, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must have their DNS server addresses manually configured.
First DNS Server Second DNS Server	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the NBG-419N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>DNS Relay</b> to have the NBG-419N act as a DNS proxy. The NBG-419N's LAN IP address displays in the field to the right (read-only). The NBG-419N tells the DHCP clients on the LAN that the NBG-419N itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG-419N, the NBG-419N forwards the query to the NBG-419N's system DNS server (configured in the <b>WAN &gt; Internet Connection</b> screen) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select <b>DNS Relay</b> for a second or third DNS server, that choice changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

Company Confidential

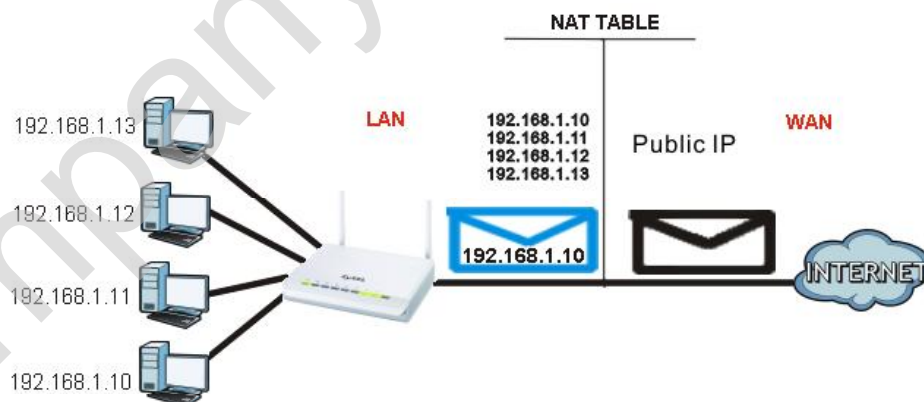
# Network Address Translation (NAT)

## 15.1 Overview

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

Each packet has two addresses – a source address and a destination address. For outgoing packets, NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The NBG-419N keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

**Figure 92** NAT Example



For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

## 15.2 What You Can Do

- Use the **General** screen (Section 15.3 on page 144) to enable NAT and set a default server.
- Use the **Application** screen (Section 15.4 on page 145) to forward incoming service requests to the server(s) on your local network.
- Use the **Advanced** screen (Section 15.5 on page 147) to change your NBG-419N's trigger port settings.

## 15.3 General NAT Screen

Use this screen to enable NAT and set a default server. Click **Network > NAT > General** to open the following screen.

**Figure 93** Network > NAT > General

The following table describes the labels in this screen.

**Table 57** Network > NAT > General

LABEL	DESCRIPTION
NAT Setup	
Enable Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).  Select the check box to enable NAT.
Default Server Setup	
Server IP Address	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the <b>Application</b> screen.  If you do not assign a <b>Default Server IP address</b> , the NBG-419N discards all packets received for ports that are not specified in the <b>Application</b> screen or remote management.



**Table 57** Network > NAT > General

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 15.4 NAT Application Screen

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

**Note:** Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG-419N's port forwarding settings, click **Network > NAT > Application**. The screen appears as shown.

**Note:** If you do not assign a **Default Server IP address** in the **NAT > General** screen, the NBG-419N discards all packets received for ports that are not specified in this screen or remote management.

Refer to [Appendix E on page 281](#) for port numbers commonly used for particular services.

**Figure 94** Network > NAT > Application

The following table describes the labels in this screen.

**Table 58** Network > NAT > Application

LABEL	DESCRIPTION
Add Application Rule	
Active	Select the check box to enable this rule and the requested service can be forwarded to the host with a specified internal IP address.  Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a name (of up to 31 printable characters) to identify this rule in the first field next to <b>Service Name</b> . Otherwise, select a predefined service in the second field next to <b>Service Name</b> . The predefined service name and port number(s) will display in the <b>Service Name</b> and <b>Port</b> fields.
Port	Type a port number(s) to define the service to be forwarded to the specified server.  To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20.  To specify two or more non-consecutive port numbers, separate them by a comma without spaces, such as 123,567.
Server IP Address	Type the IP address of the server on your LAN that receives packets from the port(s) specified in the <b>Port</b> field.
Application Rules Summary	
#	This is the number of an individual port forwarding server entry.
Active	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Port	This field displays the port number(s).

**Table 58** Network > NAT > Application (continued)

LABEL	DESCRIPTION
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the <b>Edit</b> icon to display and modify an existing rule setting in the fields under <b>Add Application Rule</b> . Click the <b>Remove</b> icon to delete a rule.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 15.5 NAT Advanced Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The NBG-419N records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NBG-419N's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG-419N forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

To change your NBG-419N's trigger port settings, click **Network > NAT > Advanced**. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

**Figure 95** Network > NAT > Advanced

The screenshot shows the 'Advanced' tab of the NAT configuration page. It features a table titled 'Port Triggering Rules' with 12 rows. Each row contains a rule index number (1-12), a name field, and two sets of port range fields: 'Incoming' (Start Port and End Port) and 'Trigger' (Start Port and End Port). Below the table are 'Apply' and 'Reset' buttons.

#	Name	Incoming		Trigger	
		Port	End Port	Port	End Port
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

The following table describes the labels in this screen.

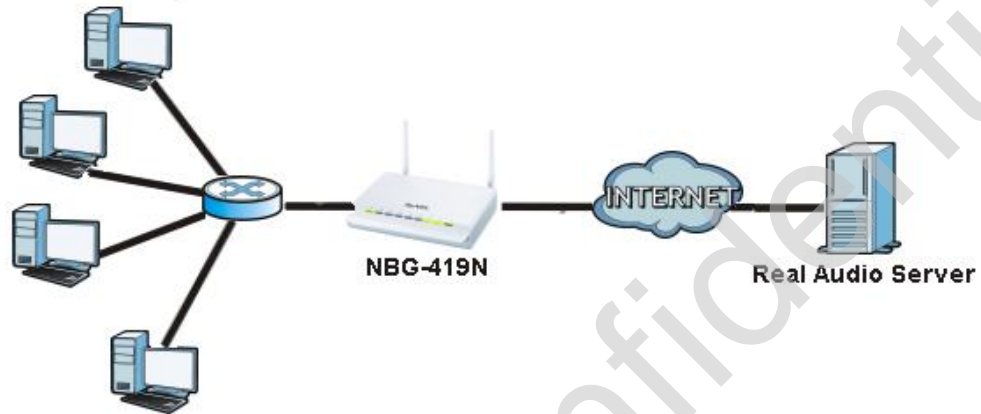
**Table 59** Network > NAT > Advanced

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The NBG-419N forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the NBG-419N to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 15.5.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

**Figure 96** Trigger Port Forwarding Process: Example  
Jane's computer



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the NBG-419N to record Jane's computer IP address. The NBG-419N associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The NBG-419N forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The NBG-419N times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

### 15.5.2 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is going coming from inside the NBG-419N and going to the outside.

If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

Company Confidential

## Dynamic DNS

### 16.1 Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

### 16.2 What You Can Do

Use the **Dynamic DNS** screen ([Section 16.4 on page 152](#)) to enable DDNS and configure the DDNS settings on the NBG-419N.

### 16.3 What You Need To Know

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

## 16.4 Dynamic DNS Screen

To change your NBG-419N's DDNS, click **Network > DDNS**. The screen appears as shown.

**Figure 97** Network > DDNS

The following table describes the labels in this screen.

**Table 60** Network > DDNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



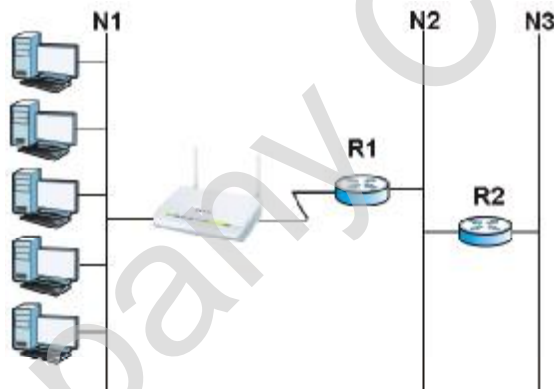
# Static Route

## 17.1 Overview

This chapter shows you how to configure static routes for your NBG-419N.

Each remote node specifies only the network to which the gateway is directly connected, and the NBG-419N has no knowledge of the networks beyond. For instance, the NBG-419N knows about network N2 in the following figure through remote node Router 1. However, the NBG-419N is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the NBG-419N about the networks beyond the remote nodes.

**Figure 98** Example of Static Routing Topology



## 17.2 What You Can Do

Use the **IP Static Route** screen ([Section 17.3 on page 154](#)) to view, add and delete routes.

## 17.3 IP Static Route Screen

Click **Network > Static Route** to open the **IP Static Route** screen.

**Figure 99** Network > Static Route

No.	Active	Name	Destination	Gateway	Metric	Delete
1	🟡	default	255.255.255.255	0.0.0.0	0	
2	🟡	default	239.255.255.250	0.0.0.0	0	
3	🟡	default	172.23.31.0	0.0.0.0	0	
4	🟡	default	192.168.3.0	0.0.0.0	0	
5	🟡	default	239.0.0.0	0.0.0.0	0	
6	🟡	default	0.0.0.0	172.23.31.254	1	

The following table describes the labels in this screen.

**Table 61** Network > Static Route

LABEL	DESCRIPTION
Static Routing Settings	
Route Name	Enter a the name that describes or identifies this route.
Destination IP Address	Enter the IP network address of the final destination.
IP Subnet Netmask	This is the subnet to which the route's final destination belongs.
Gateway IP Address	Enter the the IP address of the gateway.
Metric	Assign a number to identify the route.
Add Rule	Click this to add the IP static route.
Application Rules Summary	
No.	This is the number of an individual static route.
Active	The rules are always on and this is indicated by the icon.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.

**Table 61** Network > Static Route

LABEL	DESCRIPTION
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	This is the number assigned to the route.
Delete	Click the Delete icon to remove a static route from the NBG-419N. A window displays asking you to confirm that you want to delete the route.

Company Confidential

## 18.1 Overview

Routing Information Protocol (RIP) is an interior or intra-domain routing protocol that uses distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.

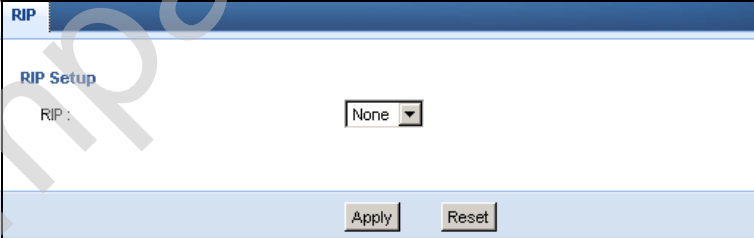
## 18.2 What You Can Do

Use the **RIP** screen ([Section 18.3 on page 157](#)) to enable RIPv1 or RIPv2, which are LAN broadcast protocols.

## 18.3 RIP Screen

Use this screen to enable RIPv1 or RIPv2, which are LAN broadcast protocols. Click **Network > RIP**. The screen appears as shown.

**Figure 100** Network > RIP



RIP Setup

RIP: None

Apply Reset

The following table describes the labels in this screen.

**Table 62** Network > RIP

LABEL	DESCRIPTION
RIP	Select the <b>RIPv1</b> or <b>RIPv2</b> you want the NBG-419N to use. Otherwise select <b>None</b> .
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

---

# PART III

## Security

---

Firewall (161)

Content Filter (167)

Company Confidential



## 19.1 Overview

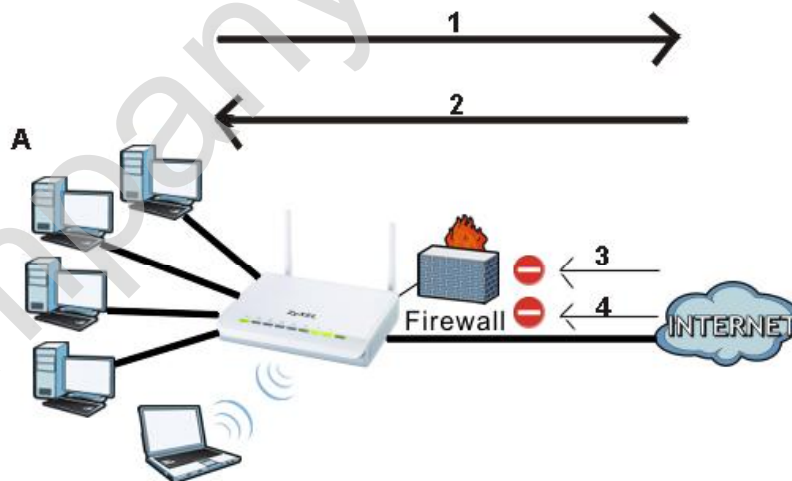
This chapter shows you how to enable and configure the firewall that protects your NBG-419N and your LAN from unwanted or malicious traffic.

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

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

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

**Figure 101** Default Firewall Action



## 19.2 What You Can Do

- Use the **General** (Section 19.4 on page 163) screen to enable or disable the NBG-419N's firewall.
- Use the **Services** screen (Section 19.5 on page 163) screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

## 19.3 What You Need To Know

The NBG-419N's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is designed to protect against Denial of Service (DoS) attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The NBG-419N's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG-419N can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The NBG-419N is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

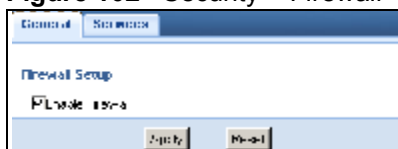
The NBG-419N has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

## 19.4 General Firewall Screen

Use this screen to enable or disable the NBG-419N's firewall, and set up firewall logs. Click **Security** > **Firewall** to open the **General** screen.

**Figure 102** Security > Firewall > General



The following table describes the labels in this screen.

**Table 63** Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The NBG-419N performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click <b>Apply</b> to save the settings.
Reset	Click <b>Reset</b> to start configuring this screen again.

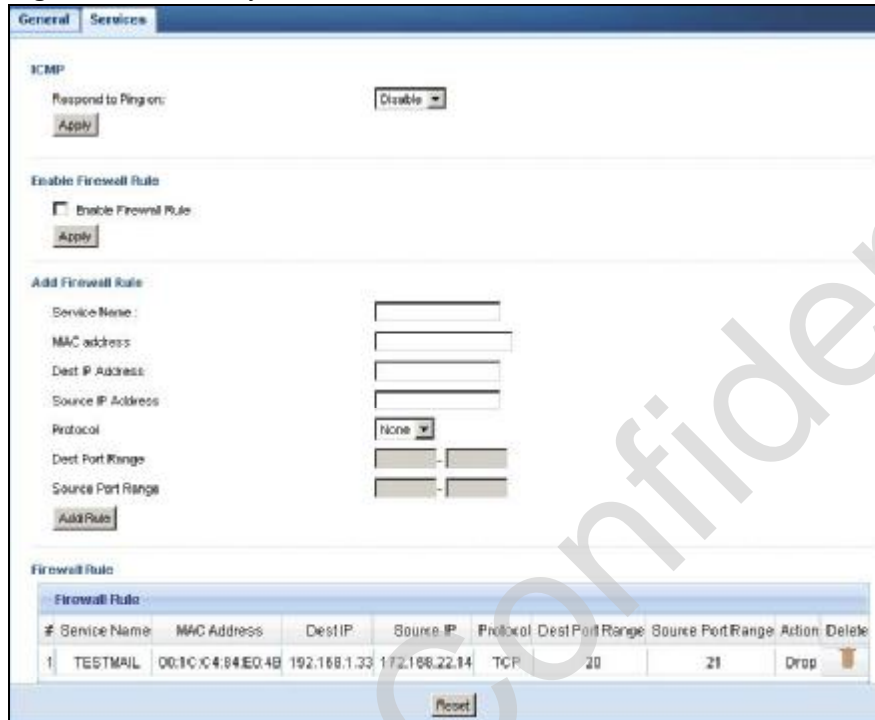
## 19.5 Services Screen

If an outside user attempts to probe an unsupported port on your NBG-419N, an ICMP response packet is automatically returned. This allows the outside user to know the NBG-419N exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG-419N when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Click **Security > Firewall > Services**. The screen appears as shown next.

**Figure 103** Security > Firewall > Services



The following table describes the labels in this screen.

**Table 64** Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The NBG-419N will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Otherwise select <b>LAN &amp; WAN</b> to reply to all incoming LAN and WAN Ping requests.
Apply	Click <b>Apply</b> to save the settings.
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see <b>Add Firewall Rule</b> below)
Apply	Click <b>Apply</b> to save the settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.

**Table 64** Security > Firewall > Services

LABEL	DESCRIPTION
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering.  The NBG-419N applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service.  The NBG-419N applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol ( <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> or <b>None</b> ) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click <b>Add</b> to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC Address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP Address	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP Address	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol ( <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> or <b>None</b> ) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	<b>Drop</b> - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click this to remove the firewall rule.
Reset	Click <b>Reset</b> to start configuring this screen again.

See [Appendix E on page 281](#) for commonly used services and port numbers.

Company Confidential

# Content Filter

## 20.1 Overview

This chapter provides a brief overview of content filtering using the embedded web GUI.

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering is the ability to block certain web features or specific URL keywords.

## 20.2 What You Can Do

Use the **Content Filter** ([Section 20.4 on page 168](#)) screen to restrict web features, add keywords for blocking and designate a trusted computer.

## 20.3 What You Need To Know

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages.

### 20.3.1 Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

#### Restrict Web Features

The NBG-419N can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.

### Keyword Blocking URL Checking

The NBG-419N checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), the domain name is [www.zyxel.com.tw](http://www.zyxel.com.tw).

The file path is the characters that come after the first slash in the URL. For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), the file path is [news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php).

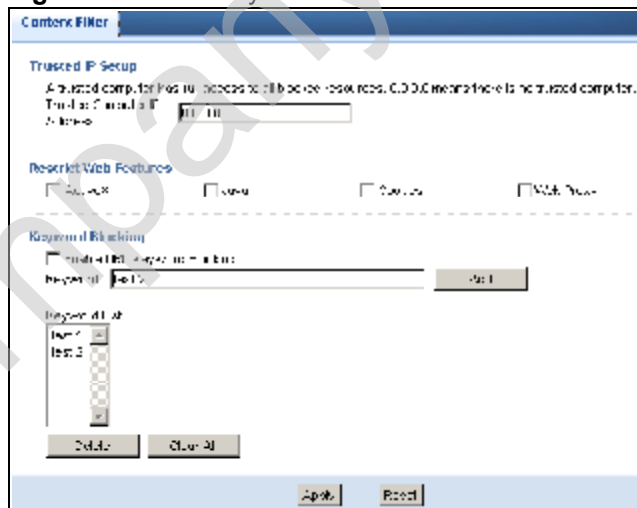
Since the NBG-419N checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), the NBG-419N would find "tw" in the domain name ([www.zyxel.com.tw](http://www.zyxel.com.tw)). It would also find "news" in the file path ([news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php)) but it would not find "tw/news".

## 20.4 Content Filter Screen

Use this screen to restrict web features, add keywords for blocking and designate a trusted computer.

Click **Security** > **Content Filter** to open the **Content Filter** screen.

**Figure 104** Security > Content Filter > Content Filter





The following table describes the labels in this screen.

**Table 65** Security > Content Filter > Content Filter

LABEL	DESCRIPTION
Trusted IP Setup	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering.  Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The NBG-419N can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL <a href="http://www.website.com/bad.html">http://www.website.com/bad.html</a> would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click <b>Add</b> after you have typed a keyword.  Repeat this procedure to add other keywords. Up to 64 keywords are allowed.  When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click <b>Delete</b> to remove it. The keyword disappears from the text box after you click <b>Apply</b> .
Clear All	Click this button to remove all of the listed keywords.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh

Company Confidential

---

# PART IV

## Management

---

Bandwidth Management (173)

Remote Management (183)

Universal Plug-and-Play (UPnP) (187)

Company Confidential

# Bandwidth Management

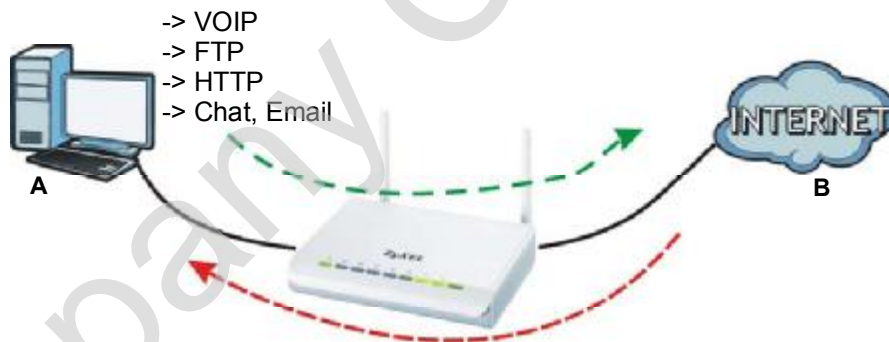
## 21.1 Overview

This chapter contains information about configuring bandwidth management and editing rules.

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application.

In the figure below, uplink traffic goes from the LAN device (**A**) to the WAN device (**B**). Bandwidth management is applied before sending the packets out to the WAN. Downlink traffic comes back from the WAN device (**B**) to the LAN device (**A**). Bandwidth management is applied before sending the traffic out to LAN.

**Figure 105** Bandwidth Management Example



You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to individual applications (like VoIP, Web, FTP, and E-mail for example).

## 21.2 What You Can Do

- Use the **General** screen ([Section 21.4 on page 174](#)) to enable bandwidth management and assign bandwidth values.

- Use the **Advanced** screen ([Section 21.5 on page 175](#)) to configure bandwidth managements rule for the pre-defined services and applications.
- Use the **Monitor** screen ([Section 21.6 on page 180](#)) to view the amount of network bandwidth that applications running in the network are using.

## 21.3 What You Need To Know

The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen ([Section 21.5 on page 175](#)).

The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen [Section 21.5 on page 175](#).

## 21.4 General Screen

Use this screen to have the NBG-419N apply bandwidth management.

Click **Management > Bandwidth MGMT** to open the bandwidth management **General** screen.

**Figure 106** Management > Bandwidth Management > General



The following table describes the labels in this screen.

**Table 66** Management > Bandwidth Management > General

LABEL	DESCRIPTION
Enable Bandwidth Management	<p>This field allows you to have NBG-419N apply bandwidth management.</p> <p>Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule.</p> <p>Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.</p>
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 21.5 Advanced Screen

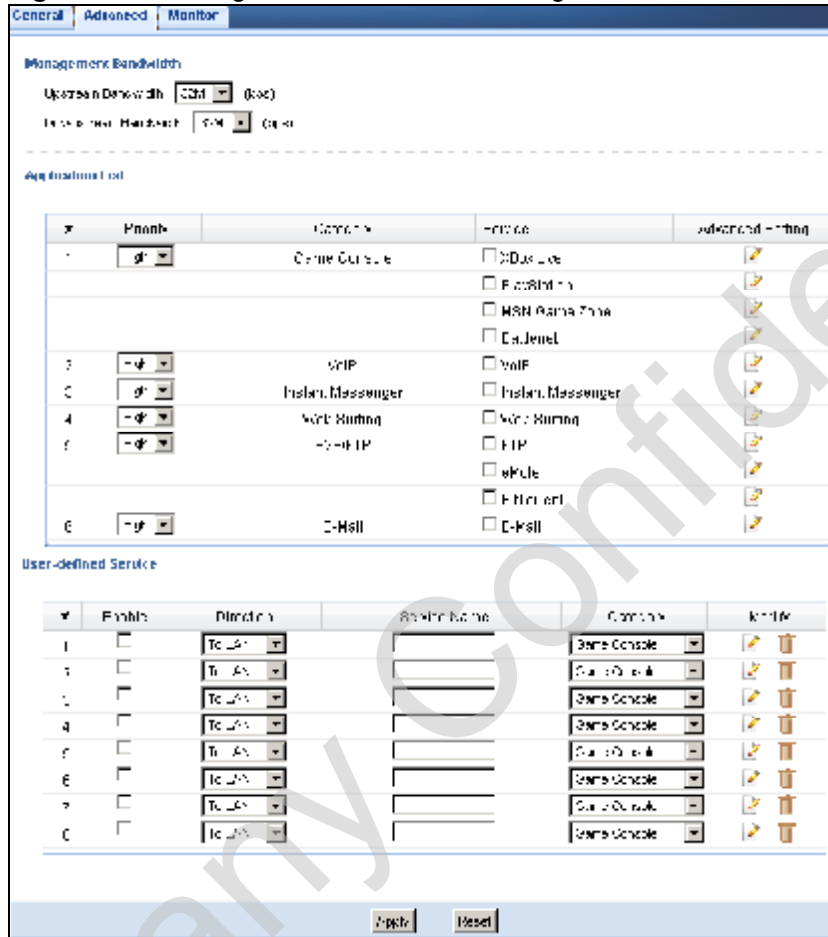
Use this screen to configure bandwidth management rules for the pre-defined services or applications.

You can also use this screen to configure bandwidth management rule for other services or applications that are not on the pre-defined list of NBG-419N. Additionally, you can define the source and destination IP addresses and port for a service or application.

Note: The two tables shown in this screen can be configured and applied at the same time.

Click **Management > Bandwidth Management > Advanced** to open the bandwidth management **Advanced** screen.

**Figure 107** Management > Bandwidth Management > Advanced



The following table describes the labels in this screen.

**Table 67** Management > Bandwidth Management > Advanced

LABEL	DESCRIPTION
Management Bandwidth	
Upstream Bandwidth	Select the total amount of bandwidth (from 64 Kilobits to 32 Megabits) that you want to dedicate to uplink traffic. This is traffic from LAN/WLAN to WAN.
Downstream Bandwidth	Select the total amount of bandwidth (from 64 Kilobits to 32 Megabits) that you want to dedicate to uplink traffic. This is traffic from WAN to LAN/WLAN.
Application List	Use this table to allocate specific amounts of bandwidth based on a pre-defined service.



**Table 67** Management > Bandwidth Management > Advanced (continued)

LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Priority	Select a priority from the drop down list box. Choose <b>High</b> , <b>Mid</b> or <b>Low</b> . <ul style="list-style-type: none"> <li>• <b>High</b> - Select this for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).</li> <li>• <b>Mid</b> - Select this for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.</li> <li>• <b>Low</b> - Select this for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.</li> </ul>
Category	This is the category where a service belongs.
Service	This is the name of the service.  Select the check box to have the NBG-419N apply this bandwidth management rule.
Advanced Setting	Click the <b>Edit</b> icon to open the <b>Rule Configuration</b> screen where you can modify the rule.
User-defined Service	Use this table to allocate specific amounts of bandwidth to specific applications or services you specify.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG-419N apply this bandwidth management rule.
Direction	Select <b>LAN</b> to apply bandwidth management to traffic from WAN to LAN.  Select <b>WAN</b> to apply bandwidth management to traffic from LAN/WLAN to WAN.  Select <b>WLAN</b> to apply bandwidth management to traffic from WAN to WLAN.
Service Name	Enter a descriptive name for the bandwidth management rule.
Category	This is the category where a service belongs.
Modify	Click the <b>Edit</b> icon to open the <b>Rule Configuration</b> screen. Modify an existing rule or create a new rule in the <b>Rule Configuration</b> screen. See <a href="#">Section 21.5.2 on page 179</a> for more information.  Click the <b>Remove</b> icon to delete a rule.
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 21.5.1 Rule Configuration: Application Rule Configuration

If you want to edit a bandwidth management rule for a pre-defined service or application, click the **Edit** icon in the **Application List** table of the **Advanced** screen. The following screen displays.

**Figure 108** Bandwidth Management Rule Configuration: Application List

#	Enable	Direction	Bandwidth	Dest. Port	Source Port	Protocol
1	<input checked="" type="checkbox"/>	Out	Minimum Bandwidth	80	80	TCP
2	<input checked="" type="checkbox"/>	Out	Minimum Bandwidth	80	80	UDP
3	<input checked="" type="checkbox"/>	Out	Minimum Bandwidth	80	80	TCP
4	<input checked="" type="checkbox"/>	Out	Minimum Bandwidth	80	80	TCP
5	<input checked="" type="checkbox"/>	Out	Minimum Bandwidth	80	80	TCP
6	<input checked="" type="checkbox"/>	Out	Minimum Bandwidth	80	80	UDP

The following table describes the labels in this screen.

**Table 68** Bandwidth Management Rule Configuration: Application List

LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Enable	Select an interface's check box to enable bandwidth management on that interface.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the NBG-419N and be managed by bandwidth management.
Bandwidth	Select <b>Maximum Bandwidth</b> or <b>Minimum Bandwidth</b> and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic. See <a href="#">Appendix E on page 281</a> for some common services and port numbers.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic. See <a href="#">Appendix E on page 281</a> for some common services and port numbers.
Protocol	This is the protocol ( <b>TCP</b> , <b>UDP</b> or user-defined) used for the service.
Apply	Click <b>Apply</b> to save your customized settings.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 21.5.2 Rule Configuration: User Defined Service Rule Configuration

If you want to edit a bandwidth management rule for other applications or services, click the **Edit** icon in the **User-defined Service** table of the **Advanced** screen. The following screen displays.

**Figure 109** Bandwidth Management Rule Configuration: User-defined Service

The following table describes the labels in this screen

**Table 69** Bandwidth Management Rule Configuration: User-defined Service

LABEL	DESCRIPTION
BW Budget	Select <b>Maximum Bandwidth</b> or <b>Minimum Bandwidth</b> and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Address	Enter the IP address of the destination computer. The NBG-419N applies bandwidth management to the service or application that is entering this computer.
Destination Subnet Netmask	Enter the subnet netmask of the destination of the traffic for which the bandwidth management rule applies.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Address	Enter the IP address of the computer that initializes traffic for the application or service. The NBG-419N applies bandwidth management to traffic initiating from this computer.
Source Subnet Netmask	Enter the subnet netmask of the computer initiating the traffic for which the bandwidth management rule applies.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic.

LABEL	DESCRIPTION
Protocol	Select the protocol ( <b>TCP</b> , <b>UDP</b> , <b>User defined</b> ) for which the bandwidth management rule applies.  If you select <b>User-defined</b> , enter the protocol for which the bandwidth management rule applies. For example, ICMP for ping traffic.
Apply	Click <b>Apply</b> to save your customized settings.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

See [Appendix E on page 281](#) for commonly used services and port numbers.

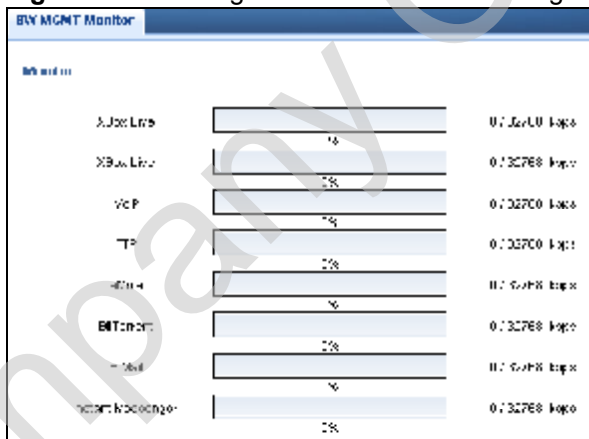
## 21.6 Monitor Screen

Use this screen to view the amount of network bandwidth that applications running in the network are using.

The bandwidth is measured in kilobits per second (kbps).

The monitor shows what kinds of applications are running in the network, the maximum kbps that each application can use, as well as the percentage of bandwidth it is using.

**Figure 110** Management > Bandwidth Management > Monitor



## 21.6.1 Predefined Bandwidth Management Services

The following is a description of some services that you can select and to which you can apply media bandwidth management in the **Management > Bandwidth Management > Advanced** screen.

**Table 70** Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail.
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail:
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.  SIP is transported primarily over UDP but can also be transported over TCP.
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by corporation and trading, that is, the client downloads the file in small pieces and share the pieces with other peers to get other half of the file.
Gaming	Online gaming services lets you play multiplayer games on the Internet via broadband technology. As of this writing, your NBG-419N supports Xbox, Playstation, Battlenet and MSN Game Zone.

Company Confidential

# Remote Management

## 22.1 Overview

This chapter provides information on the Remote Management screens.

Remote Management allows you to manage your NBG-419N from a remote location through the following interfaces:

- LAN and WAN
- LAN only
- WAN only

Note: The NBG-419N is managed using the Web Configurator.

## 22.2 What You Can Do

Use the **www** screen ([Section 22.4 on page 184](#)) to define the interface/s from which the NBG-419N can be managed remotely and specify a secure client that can manage the NBG-419N.

## 22.3 What You Need to Know

Remote management over LAN or WAN will not work when:

- 1 The IP address in the **Secured Client IP Address** field ([Section 22.4 on page 184](#)) does not match the client IP address. If it does not match, the NBG-419N will disconnect the session immediately.
- 2 There is already another remote management session. You may only have one remote management session running at one time.
- 3 There is a firewall rule that blocks it.

### 22.3.1 Remote Management and NAT

When NAT is enabled:

- Use the NBG-419N's WAN IP address when configuring from the WAN.
- Use the NBG-419N's LAN IP address when configuring from the LAN.

### 22.3.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG-419N automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

## 22.4 WWW Screen

To change your NBG-419N's remote management settings, click **Management > Remote Management > WWW**.

**Figure 111** Management > Remote Management > WWW



The following table describes the labels in this screen

**Table 71** Management > Remote Management > WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG-419N using this service.
Secured Client IP Address	Select <b>All</b> to allow all computes to access the NBG-419N. Otherwise, check <b>Selected</b> and specify the IP address of the computer that can access the NBG-419N.



LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

Company Confidential

Company Confidential

# Universal Plug-and-Play (UPnP)

## 23.1 Overview

This chapter introduces the UPnP feature in the web configurator.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

## 23.2 What You Can Do

Use the UPnP screen ([Section 23.4 on page 188](#)) to enable UPnP on your NBG-419N.

## 23.3 What You Need to Know

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

### 23.3.1 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping

- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

### 23.3.2 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NBG-419N allows multicast messages on the LAN only.

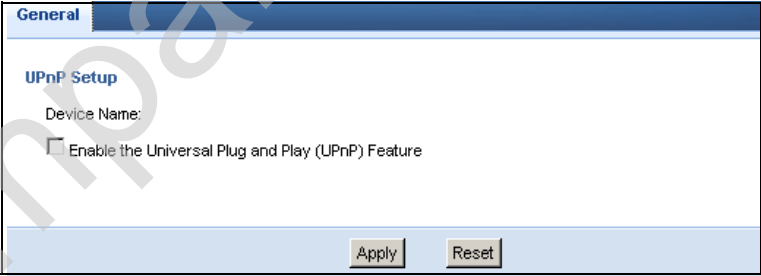
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## 23.4 UPnP Screen

Use this screen to enable UPnP on your NBG-419N.

Click **Management > UPnP** to display the screen shown next.

**Figure 112** Management > UPnP



The screenshot shows a web-based configuration page for UPnP. At the top, there is a tab labeled "General". Below the tab, the page title is "UPnP Setup". There is a label "Device Name:" followed by a text input field. Below that is a checkbox labeled "Enable the Universal Plug and Play (UPnP) Feature". At the bottom of the page, there are two buttons: "Apply" and "Reset".

The following table describes the fields in this screen.

**Table 72** Management > UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the NBG-419N's IP address (although you must still enter the password to access the web configurator).
Apply	Click <b>Apply</b> to save the setting to the NBG-419N.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 23.5 Technical Reference

The sections show examples of using UPnP.

### 23.5.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the NBG-419N.

Make sure the computer is connected to a LAN port of the NBG-419N. Turn on your computer and the NBG-419N.

#### 23.5.1.1 Auto-discover Your UPnP-enabled Network Device

- 1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.

**Figure 113** Network Connections



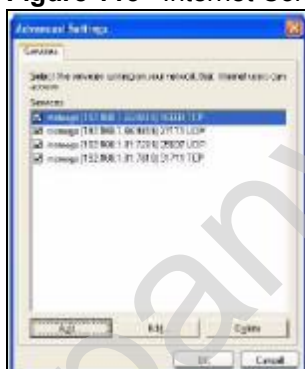
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

**Figure 114** Internet Connection Properties

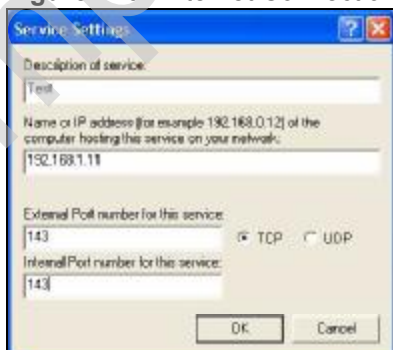


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 115** Internet Connection Properties: Advanced Settings



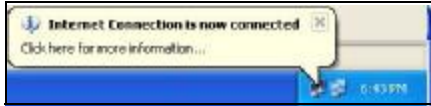
**Figure 116** Internet Connection Properties: Advanced Settings: Add



Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 5 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

**Figure 117** System Tray Icon



- 6 Double-click on the icon to display your current Internet connection status.

**Figure 118** Internet Connection Status



## 23.5.2 Web Configurator Easy Access

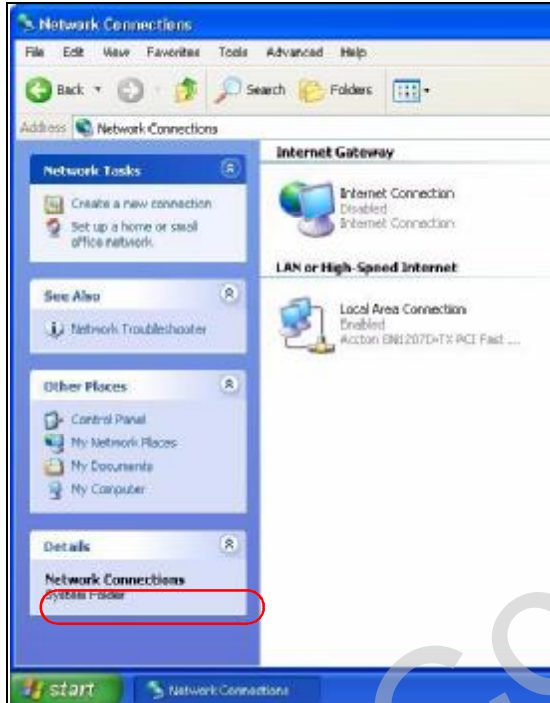
With UPnP, you can access the web-based configurator on the NBG-419N without finding out the IP address of the NBG-419N first. This comes helpful if you do not know the IP address of the NBG-419N.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

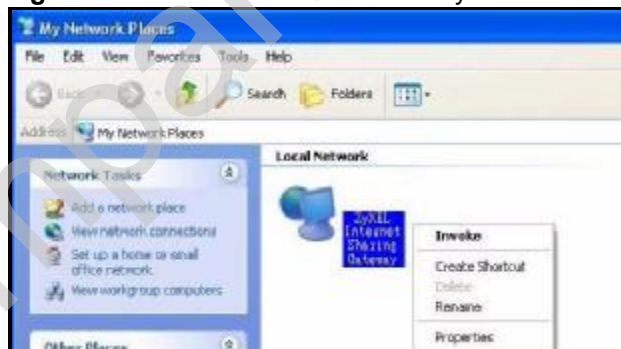
- 3 Select **My Network Places** under **Other Places**.

**Figure 119** Network Connections



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click on the icon for your NBG-419N and select **Invoke**. The web configurator login screen displays.

**Figure 120** Network Connections: My Network Places





- 6 Right-click on the icon for your NBG-419N and select **Properties**. A properties window displays with basic information about the NBG-419N.

**Figure 121** Network Connections: My Network Places: Properties: Example



Company Confidential

---

# PART V

## Maintenance and Troubleshooting

---

Maintenance (197)

Password (199)

Time (201)

Firmware Upgrade (205)

Backup/Restore (207)

Reset/Restart (211)

Sys OP Mode (213)

Troubleshooting (217)

Company Confidential

# Maintenance

## 24.1 Overview

This chapter provides information on the **Maintenance > General** screen.

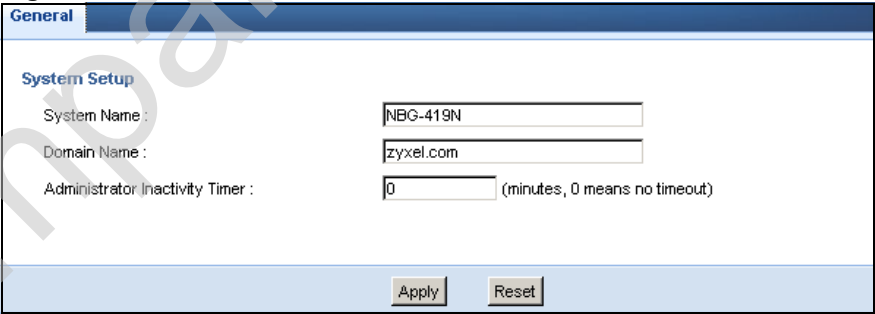
## 24.2 What You Can Do

- Use the **General** screen ([Section 24.3 on page 197](#)) to enter a name to identify the NBG-419N in the network and set the password.
- Use the **Time Setting** screen ([Section 26.3 on page 201](#)) to change your NBG-419N's time and date.

## 24.3 General Screen

Use this screen to enter a name to identify the NBG-419N in the network and set the password. Click **Maintenance > General**. The following screen displays.

**Figure 122** Maintenance > General



The screenshot shows the 'General' tab of the 'Maintenance > General' screen. The 'System Setup' section contains three input fields: 'System Name' with the value 'NBG-419N', 'Domain Name' with the value 'zyxel.com', and 'Administrator Inactivity Timer' with the value '0' and a note '(minutes, 0 means no timeout)'. At the bottom of the form are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 73** Maintenance > General

LABEL	DESCRIPTION
System Setup	
System Name	System Name is a unique name to identify the NBG-419N in an Ethernet network.
Domain Name	Enter the domain name you want to give to the NBG-419N.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 25.1 Overview

This chapter contains information about configuring general log settings and viewing the NBG-419N's logs. Refer to the appendices for example log message explanations.

The Web Configurator allows you to look at all of the NBG-419N's logs in one location.

## 25.2 What You Can Do

Use the **View Log** screen ([Section 25.4 on page 200](#)) to see the logs for the categories such as system maintenance, system errors, access control, allowed or blocked web sites, blocked web features, and so on.

## 25.3 What You Need to Know

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

## 25.4 Password Screen

Use the **View Log** screen to see the logged messages for the NBG-419N. Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Click **Maintenance > Password**.

**Figure 123** Maintenance > Password

The following table describes the labels in this screen.

**Table 74** Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your NBG-419N's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# 26

## Time

### 26.1 Overview

This chapter provides information on the **Time Setting** screens. See [Section 3.2.3 on page 39](#) for more information on how to set up the NBG-419N's date and time.

### 26.2 What You Can Do

Use the Time Setting screen ([Section 26.3 on page 201](#)) to change your NBG-419N's time and date.

### 26.3 Time Setting Screen

Use this screen to configure the NBG-419N's time based on your local time zone. To change your NBG-419N's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown.

Figure 124 Maintenance > Time

The screenshot shows the 'Time Setting' web interface. It is divided into several sections:

- Current Time and Date:** Displays 'Current Time' as 14:27:33 and 'Current Date' as 2006-07-11.
- Current Time and Date (Configuration):** Includes radio buttons for 'Manual' and 'Auto'. Under 'Manual', there are input fields for 'New Time (HH:MM:SS)' (14:27:33) and 'New Date (YYYY-MM-DD)' (2006-07-11). Under 'Auto', there is a 'Use Defined Time Server (Address):' field with the value 'Time.sidi.net:8080'.
- Time Zone Setup:** Features a 'Time Zone' dropdown menu set to '(UTC+08:00) PRC Time', a 'Daylight Savings' checkbox, and 'Start' and 'End' date and time fields.
- Buttons:** 'Apply' and 'Cancel' buttons are located at the bottom of the form.

The following table describes the labels in this screen.

**Table 75** Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG-419N. Each time you reload this page, the NBG-419N synchronizes the time with the time server.
Current Date	This field displays the date of your NBG-419N. Each time you reload this page, the NBG-419N synchronizes the date with the time server.
Current Time and Date	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .
Get from Time Server	Select this radio button to have the NBG-419N get the time and date from the time server you specified below.
Auto	Select <b>Auto</b> to have the NBG-419N automatically search for an available time server and synchronize the date and time with the time server after you click <b>Apply</b> .
User Defined Time Server Address	Select <b>User Defined Time Server Address</b> and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.

**Table 75** Maintenance > Time

LABEL	DESCRIPTION
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Daylight Savings</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, April</b> and type 2 in the <b>o'clock</b> field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Last, Sunday, October</b> and type 2 in the <b>o'clock</b> field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click <b>Apply</b> to save your changes back to the NBG-419N.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

Company Confidential

## Firmware Upgrade

### 27.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG-419N.

### 27.2 What You Can Do

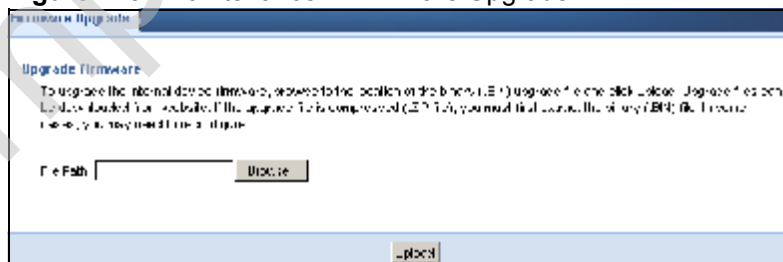
Use the **Firmware** screen (Section 27.3 on page 205) to upload firmware to your NBG-419N.

### 27.3 Firmware Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a ".bin" extension, e.g., "NBG-419N.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your NBG-419N.

**Figure 125** Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

**Table 76** Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the NBG-419N while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG-419N again.

The NBG-419N automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 126** Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware** screen.

# Backup/Restore

## 28.1 Overview

This chapter shows you how to backup, restore and reset your NBG-419N.

Backup configuration allows you to back up (save) the NBG-419N's current configuration to a file on your computer. Once your NBG-419N is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG-419N.

## 28.2 What You Can Do

Use the **Backup/Restore** screen ([Section 28.3 on page 208](#)) to view information related to factory defaults, backup configuration, and restoring configuration.

## 28.3 Configuration Screen

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**Figure 127** Maintenance > Backup/Restore

**Backup/Restore**

**Backup Configuration**

Click Backup to save the current configuration of your system to your computer.

**Restore Configuration**

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path :

**Back to Factory Defaults**

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

The following table describes the labels in this screen.

**Table 77** Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click <b>Backup</b> to save the NBG-419N's current configuration to your computer.
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.



**Table 77** Maintenance > Backup/Restore

LABEL	DESCRIPTION
Upload	<p>Click <b>Upload</b> to begin the upload process.</p> <p><b>Note:</b> Do not turn off the NBG-419N while configuration file upload is in progress.</p> <p>After you see a “configuration upload successful” screen, you must then wait one minute before logging into the NBG-419N again. The NBG-419N automatically restarts in this time causing a temporary network disconnect.</p> <p>If you see an error screen, click Back to return to the Backup/Restore screen.</p>
Reset	<p>Pressing the <b>Reset</b> button in this section clears all user-entered configuration information and returns the NBG-419N to its factory defaults.</p> <p>You can also press the <b>RESET</b> button on the rear panel to reset the factory defaults of your NBG-419N. Refer to the chapter about introducing the Web Configurator for more information on the <b>RESET</b> button.</p>

**Note:** If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG-419N IP address (192.168.1.1). See [Appendix C on page 251](#) for details on how to set up your computer’s IP address.

Company Confidential

## Reset/Restart

### 29.1 Overview

This chapter shows you how to restart your NBG-419N.

### 29.2 What You Can Do

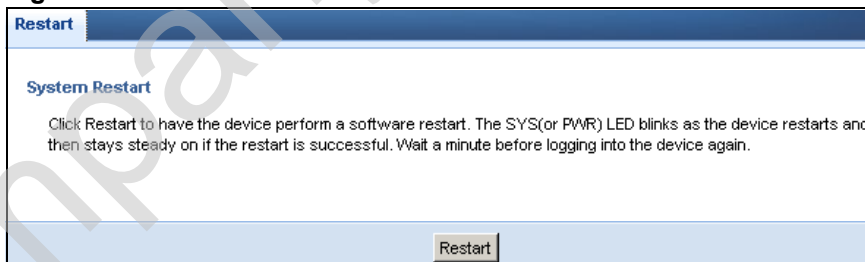
Use the **Reset/Restart** screen ([Section 29.3 on page 211](#)) to reboot the NBG-419N without turning the power off.

### 29.3 Reset/Restart Screen

System restart allows you to reboot the NBG-419N without turning the power off.

Click **Maintenance > Reset/Restart** to open the following screen.

**Figure 128** Maintenance > Reset/Restart



Click **Restart** to have the NBG-419N reboot. This does not affect the NBG-419N's configuration.

Company Confidential

## Sys OP Mode

### 30.1 Overview

The **Sys OP Mode** (System Operation Mode) function lets you configure your NBG-419N as a router, access point or Wireless ISP (WISP) client. You can choose between **Router Mode**, **Access Point Mode** and **WISP Mode** depending on your network topology and the features you require from your device.

See [Section 5.1.2 on page 49](#) for more information on which mode to choose.

### 30.2 What You Can Do

Use the **Sys OP Mode** screen ([Section 30.4 on page 215](#)) to select how you want to use your NBG-419N.

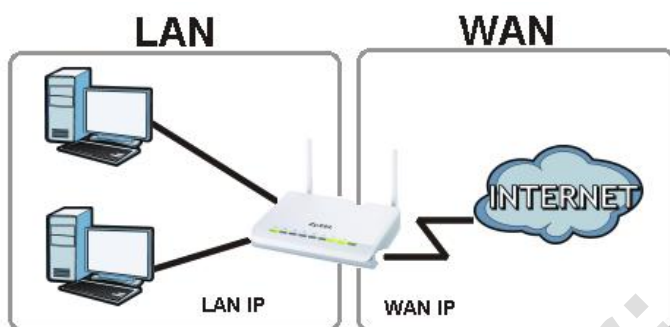
### 30.3 What You Need to Know

The following describes the device modes available in your NBG-419N.

### Router

A router connects your local network with another network, such as the Internet. The router has two IP addresses, the LAN IP address and the WAN IP address.

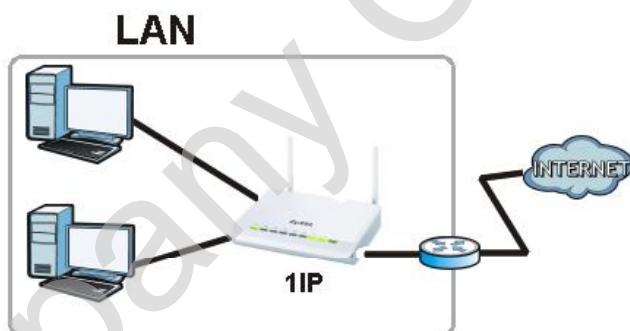
**Figure 129** LAN and WAN IP Addresses in Router Mode



### Access Point

An access point enabled all ethernet ports to be bridged together and be in the same subnet. To connect to the Internet, another device, such as a router, is required.

**Figure 130** IP Address in Access Point Mode



## WISP

A WISP client connects to an existing access point wirelessly. It acts just like a wireless client in notebooks/computers.

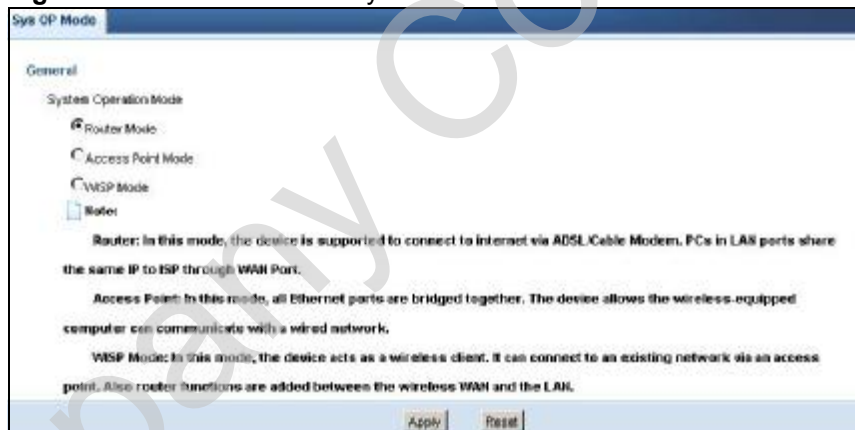
**Figure 131** IP Address in Access Point Mode



## 30.4 Sys Op Mode Screen

Use this screen to select how you want to use your NBG-419N.

**Figure 132** Maintenance > Sys OP Mode



The following table describes the labels in the **General** screen.

**Table 78** Maintenance > Sys OP Mode

LABEL	DESCRIPTION
System Operation Mode	
Router	Select <b>Router Mode</b> if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management.  You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

LABEL	DESCRIPTION
Access Point	Select <b>Access Point Mode</b> if your device bridges traffic between clients on the same network. <ul style="list-style-type: none"><li>• In Access Point mode all Ethernet ports have the same IP address.</li><li>• All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port.</li><li>• The DHCP server on your device is disabled.</li><li>• The IP address of the device on the local network is set to 192.168.1.2.</li></ul>
WISP Mode	Select <b>WISP Mode</b> if your device needs a wireless client to connect to an existing access point. <ul style="list-style-type: none"><li>• You cannot configure Wireless LAN settings (including WPS) and scheduling in the WISP mode.</li><li>• The IP address of the device on the local network is the same as the IP address given to the NBG-419N while in router mode (default is 192.168.1.1).</li></ul>
Apply	Click <b>Apply</b> to save your settings.
Reset	Click <b>Reset</b> to return your settings to the default ( <b>Router</b> )

Note: If you select the incorrect System Operation Mode you may not be able to connect to the Internet.



# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [NBG-419N Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG-419N to Its Factory Defaults](#)
- [Wireless Router/AP Troubleshooting](#)

## 31.1 Power, Hardware Connections, and LEDs

---

The NBG-419N does not turn on. None of the LEDs turn on.

---

- 1 Make sure you are using the power adaptor or cord included with the NBG-419N.
- 2 Make sure the power adaptor or cord is connected to the NBG-419N and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG-419N.
- 4 If the problem continues, contact the vendor.

---

One of the LEDs does not behave as expected.

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5 on page 22](#).
- 2 Check the hardware connections. See the Quick Start Guide.

- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the power adaptor to the NBG-419N.
- 5 If the problem continues, contact the vendor.

## 31.2 NBG-419N Access and Login

---

I don't know the IP address of my NBG-419N.

---

- 1 The default IP address is **192.168.1.1**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the NBG-419N by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the NBG-419N (it depends on the network), so enter this IP address in your Internet browser. Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your NBG-419N's IP address is available in the **Device Information** table.
  - If the **DHCP** setting under **LAN information** is **None**, your device has a fixed IP address.
  - If the **DHCP** setting under **LAN information** is **Client**, then your device receives an IP address from a DHCP server on the network.
- 3 If your NBG-419N is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
- 4 Reset your NBG-419N to change all settings back to their default. This means your current settings are lost. See [Section 31.4 on page 221](#) in the **Troubleshooting** for information on resetting your NBG-419N.

---

I forgot the password.

---

- 1 The default password is **1234**.

- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 31.4 on page 221](#).

---

**I cannot see or access the [Login](#) screen in the Web Configurator.**

---

- 1 Make sure you are using the correct IP address.
  - The default IP address is [192.168.1.1](#).
  - If you changed the IP address ([Section 13.4 on page 137](#)), use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I don't know the IP address of my NBG-419N](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix A on page 233](#).
- 4 Make sure your computer is in the same subnet as the NBG-419N. (If you know that there are routers between your computer and the NBG-419N, skip this step.)
  - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 14.3 on page 139](#).
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG-419N. See [Appendix B on page 241](#).
- 5 Reset the device to its factory defaults, and try to access the NBG-419N with the default IP address. See [Section 28.3 on page 208](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestion**

- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

---

**I can see the [Login](#) screen, but I cannot log in to the NBG-419N.**

---

- 1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

- 2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG-419N.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 31.4 on page 221](#).

## 31.3 Internet Access

---

I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
  - Go to Network > Wireless LAN > General > WDS and check if the NBG-419N is set to bridge mode. Select **Disable** and try to connect to the Internet again.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 Go to Maintenance > Sys OP Mode > General. Check your System Operation Mode setting.
  - Select **Router** if your device routes traffic between a local network and another network such as the Internet.
  - Select **Access Point** if your device bridges traffic between clients on the same network.
- 6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG-419N), but my Internet connection is not available anymore.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.5 on page 22](#).
- 2 Reboot the NBG-419N.
- 3 If the problem continues, contact your ISP.

---

### The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.5 on page 22](#). If the NBG-419N is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving the NBG-419N closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Reboot the NBG-419N.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.
- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

## 31.4 Resetting the NBG-419N to Its Factory Defaults

If you reset the NBG-419N, you lose all of the changes you have made. The NBG-419N re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

---

You will lose all of your changes when you push the **RESET** button.

---

To reset the NBG-419N,

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the NBG-419N.
- 3 Press the **RESET** button for longer than five seconds to set the NBG-419N back to its factory-default configurations.

If the NBG-419N restarts automatically, wait for the NBG-419N to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG-419N does not restart automatically, disconnect and reconnect the NBG-419N's power. Then, follow the directions above again.

## 31.5 Wireless Router/AP Troubleshooting

---

I cannot access the NBG-419N or ping any computer from the WLAN (wireless AP or router).

---

- 1 Make sure the wireless LAN is enabled on the NBG-419N
- 2 Make sure the wireless adapter on the wireless station is working properly.
- 3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the NBG-419N.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG-419N.
- 5 Check that both the NBG-419N and your wireless station are using the same wireless and wireless security settings.
- 6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the NBG-419N.
- 7 Make sure you allow the NBG-419N to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User's Guide for more information.
- to select Router Mode.

---

I set up URL keyword blocking, but I can still access a website that should be blocked.

---

Make sure that you select the **Enable URL Keyword Blocking** check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the **Keyword List**.

If a keyword that is listed in the **Keyword List** is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filter chapter.

---

I can access the Internet, but I cannot open my network folders.

---

In the Network > LAN > Advanced screen, make sure **Allow between LAN and WAN** is checked. This is not checked by default to keep the LAN secure.

If you still cannot access a network folder, make sure your account has access rights to the folder you are trying to open.

---

I can access the Web Configurator after I switched to AP mode.

---

When you change from router mode to AP mode, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

Refer to [Appendix C on page 251](#) for instructions on how to change your computer's IP address.

Company Confidential



## Product Specifications

The following tables summarize the NBG-419N's hardware and firmware features.

**Table 79** Hardware Features

Dimensions (W x D x H)	162 mm x 115 mm x 33 mm
Weight	252 g
Power Specification	Input: 100~240 V AC, 50~60 Hz Output: 12 V DC 1A
Ethernet ports	Auto-negotiating: 10 Mbps, 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
4-5 Port Switch	A combination of switch and router makes your NBG-419N a cost-effective and viable network solution. You can add up to four computers to the NBG-419N without the cost of a hub when connecting to the Internet through the WAN port. You can add up to five computers to the NBG-419N when you connect to the Internet in AP mode. Add more than four computers to your LAN by using a hub.
LEDs	PWR, LAN1-4, WAN, WLAN, WPS
Reset Button	The reset button is built into the rear panel. Use this button to restore the NBG-419N to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
WPS button	Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection.
Wireless Switch	Turn on or turn off the wireless function of the NBG-419N using this switch. There is no need to go into the Web Configurator.
Antenna	The NBG-419N is equipped with two 2dBi (2.4GHz) detachable antennas to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0° C ~ 40° C / 32°F ~ 104°F Humidity: 20% ~ 90%
Storage Environment	Temperature: -30° C ~ 70° C / -22°F ~ 158°F Humidity: 20% ~ 95%

**Table 80** Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1 (router) 192.168.1.2. (AP)
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
Wireless Interface	Wireless LAN
Default Wireless SSID	ZyXEL
Default Wireless DHCP Pool Size	Wireless LAN: Same as LAN (32 from 192.168.1.33 to 192.168.1.64)
Device Management	Use the Web Configurator to easily configure the rich range of features on the NBG-419N.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the NBG-419N wirelessly. Enable wireless security ( WPA(2)-PSK) and/or MAC filtering to protect your wireless network.  <b>Note:</b> The NBG-419N may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator to put it on the NBG-419N.  <b>Note:</b> Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the NBG-419N's configuration and put it back on the NBG-419N later if you decide you want to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the NBG-419N for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.

**Table 80** Firmware Features

FEATURE	DESCRIPTION
Content Filter	The NBG-419N blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering.  You can also subscribe to category-based content filtering that allows your NBG-419N to check web sites against an external database.
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the NBG-419N.
Wireless LAN Scheduler	You can schedule the times the Wireless LAN is enabled/disabled.
Time and Date	Get the current time and date from an external server when you turn on your NBG-419N. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the NBG-419N assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, <a href="http://www.zyxel.com">www.zyxel.com</a> for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The NBG-419N supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Logging	Use logs for troubleshooting. You can view logs in the Web Configurator.
PPPoE	PPPoE mimics a dial-up Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The NBG-419N supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The NBG-419N can communicate with other UPnP enabled devices in a network.

## 32.1 Wall-mounting Instructions

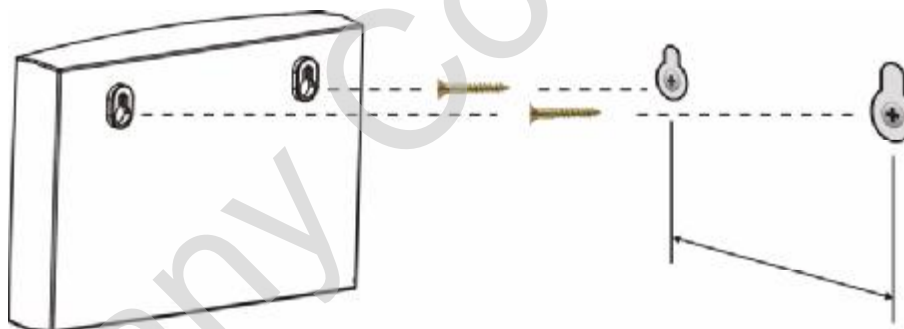
Complete the following steps to hang your NBG-419N on a wall.

- 1 Select a position free of obstructions on a sturdy wall.
- 2 Drill two holes for the screws.

**Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.**

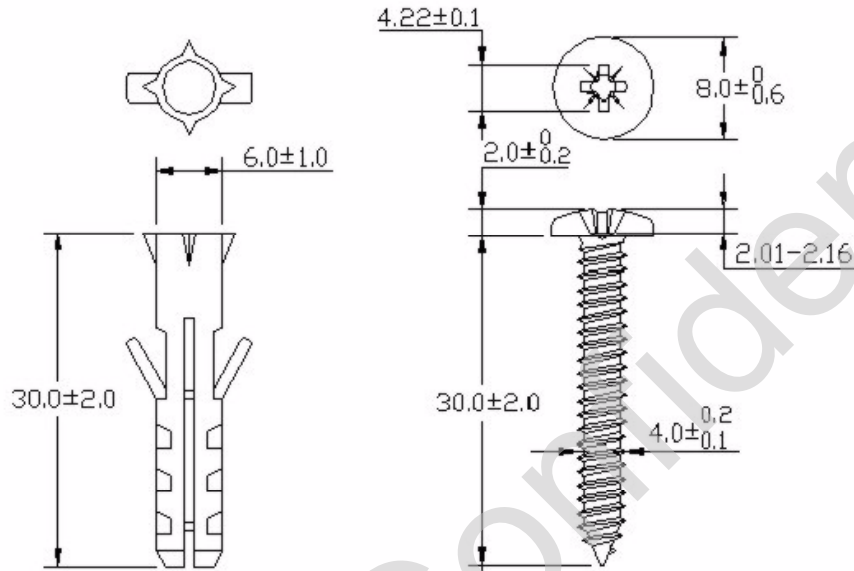
- 3 Do not insert the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the NBG-419N with the connection cables.
- 5 Align the holes on the back of the NBG-419N with the screws on the wall. Hang the NBG-419N on the screws.

**Figure 133** Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

**Figure 134** Masonry Plug and M4 Tap Screw



Company Confidential

---

# PART VI

## Appendices and Index

---

Pop-up Windows, JavaScripts and Java  
Permissions (233)

IP Addresses and Subnetting (241)

Setting up Your Computer's IP Address  
(251)

Wireless LANs (269)

Common Services (281)

Legal Information (285)

Index (293)

Company Confidential



# Pop-up Windows, JavaScripts and Java Permissions

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

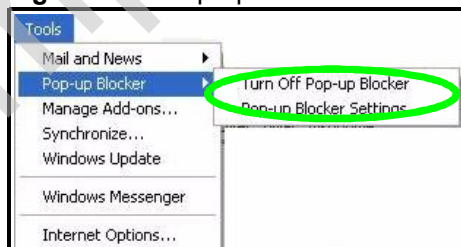
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

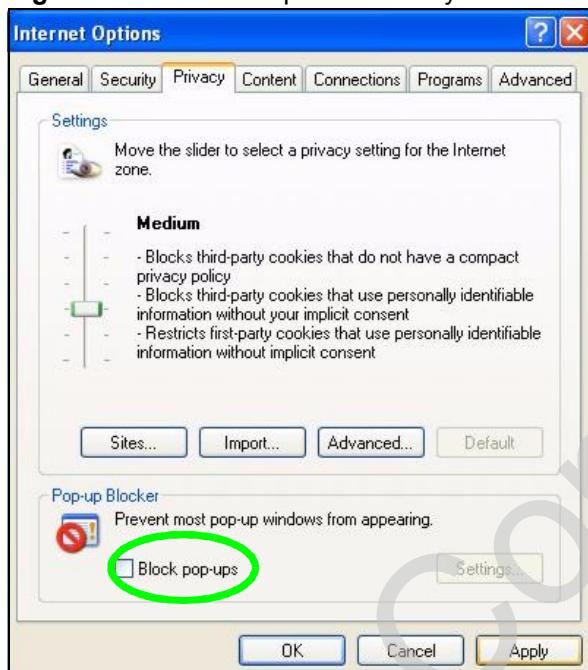
Figure 135 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 136** Internet Options: Privacy



- 3 Click **Apply** to save this setting.

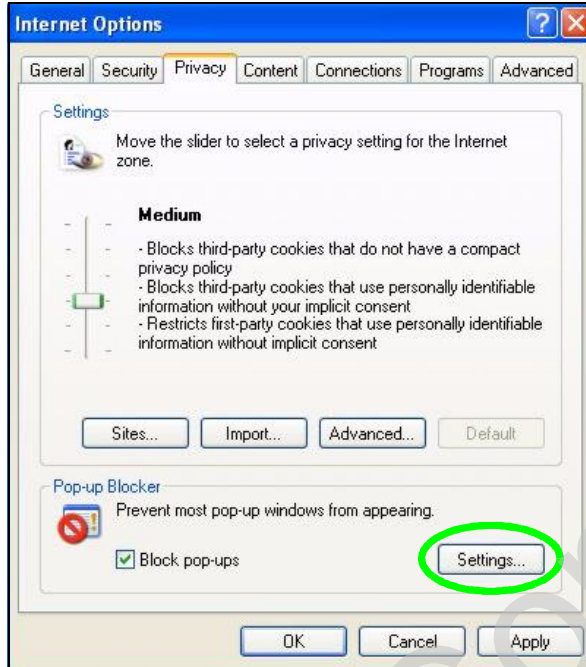
### Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.

- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

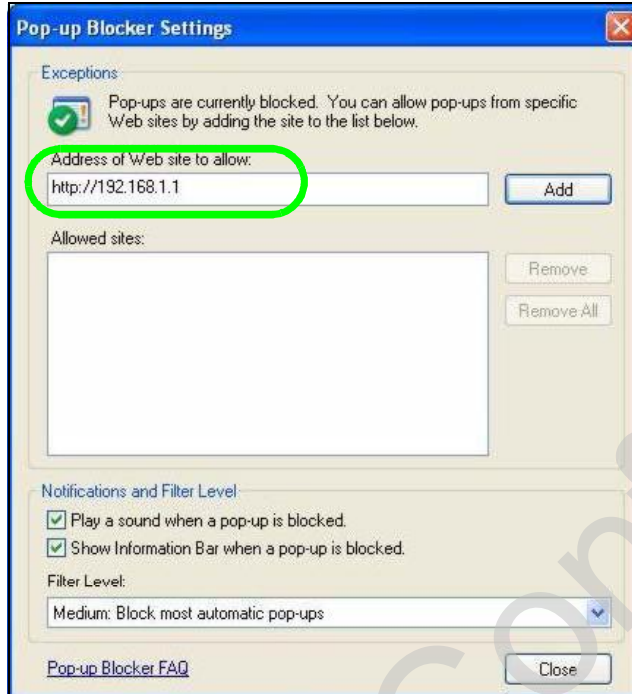
**Figure 137** Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, `http://192.168.167.1`.

- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 138** Pop-up Blocker Settings



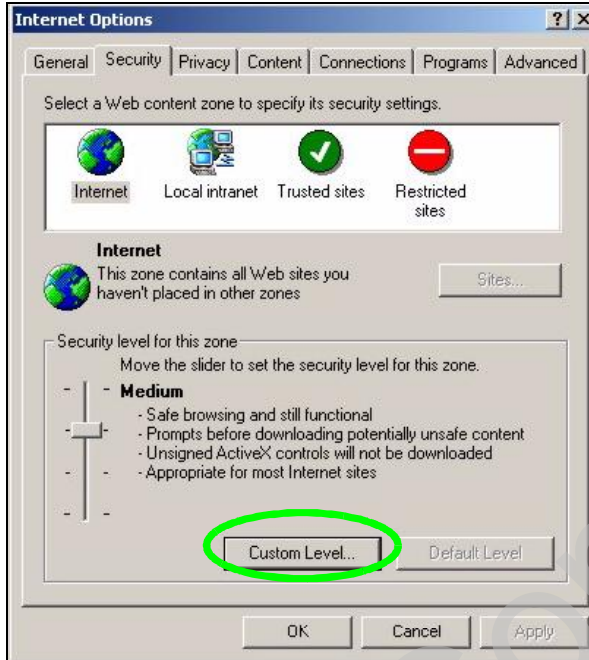
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScripts

If pages of the Web Configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

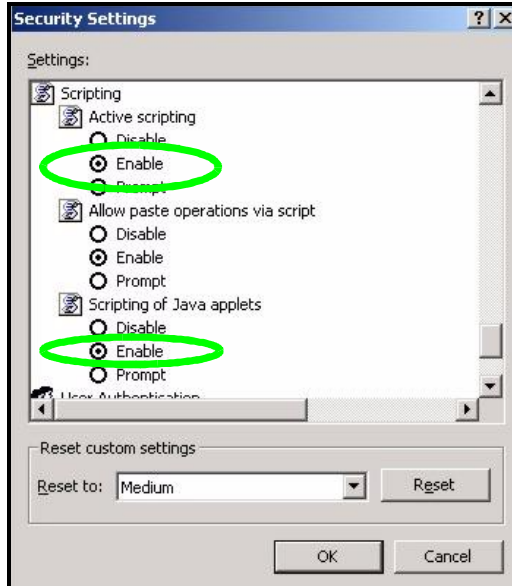
**Figure 139** Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

**Figure 140** Security Settings - Java Scripting

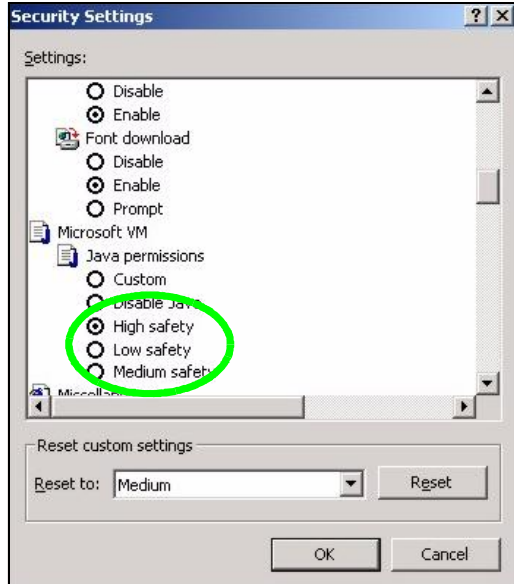


## Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

**Figure 141** Security Settings - Java

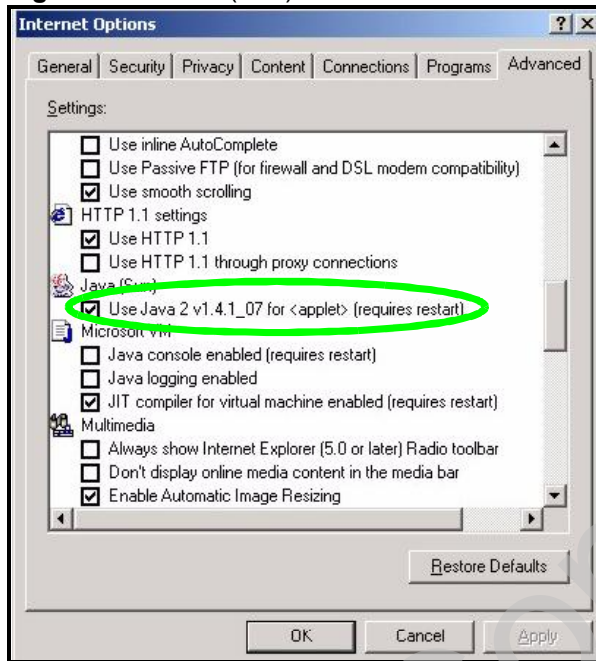


### JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

- 3 Click **OK** to close the window.

**Figure 142** Java (Sun)





# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

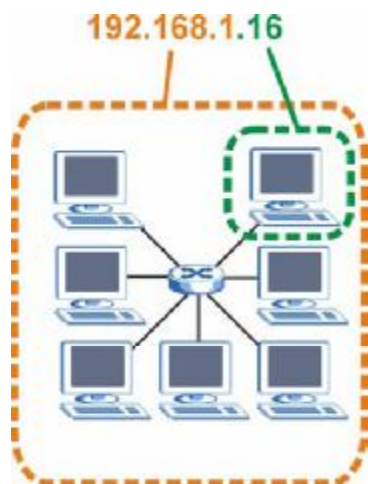
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 143** Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 81** Subnet Mask - Identifying Network Number

	<b>1ST OCTET: (192)</b>	<b>2ND OCTET: (168)</b>	<b>3RD OCTET: (1)</b>	<b>4TH OCTET (2)</b>
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	<b>11111111</b>	<b>11111111</b>	<b>11111111</b>	00000000

**Table 81** Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
Network Number	<b>11000000</b>	<b>10101000</b>	<b>00000001</b>	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 82** Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

### Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 83** Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 84** Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

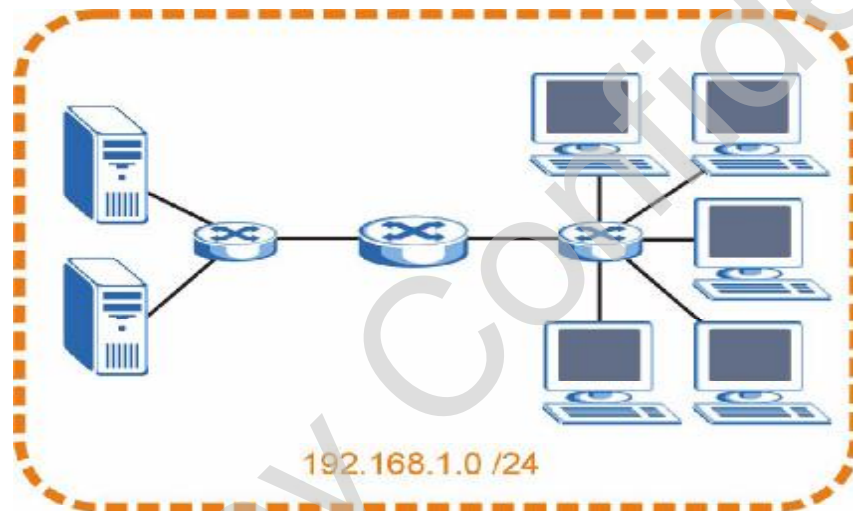
## Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of  $2^8 - 2$  or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 144** Subnetting Example: Before Subnetting

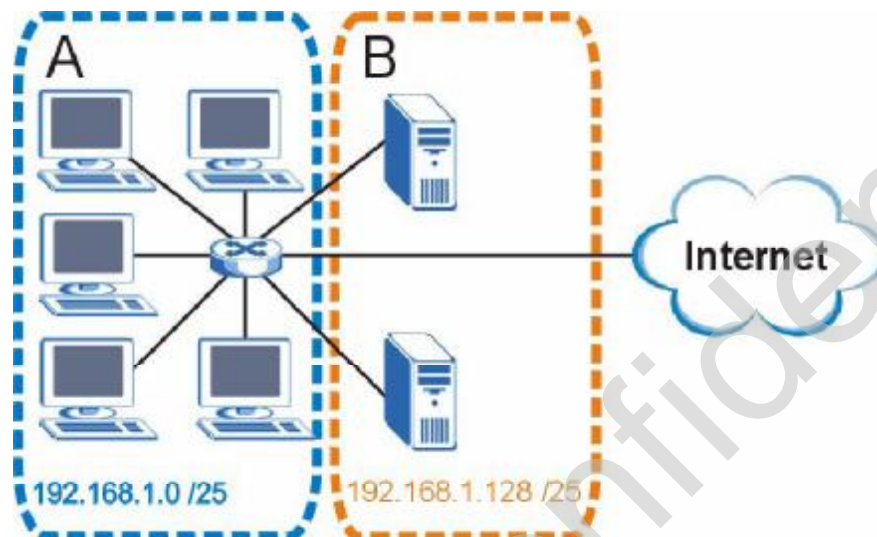


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 145** Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of  $2^7 - 2$  or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving  $2^6 - 2$  or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 85** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 86** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	<b>01000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 87** Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	<b>10000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 88** Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	<b>11000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>

**Table 88** Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 89** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 90** 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1



The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 91** 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

## Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. 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. You must also enable Network Address Translation (NAT) on the NBG-419N.

Once you have decided on the network number, pick an IP address for your NBG-419N that is easy to remember (for instance, 192.168.1.1) 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 NBG-419N 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 NBG-419N unless you are instructed to do otherwise.

### Private IP Addresses

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

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

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

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

# C

## Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

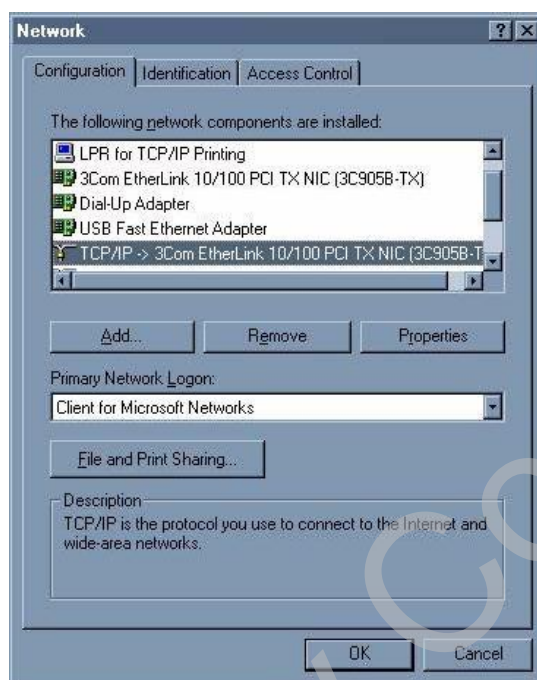
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

## Windows 95/98/Me

Click **Start, Settings, Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 146** Windows 95/98/Me: Network: Configuration



### Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.

- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

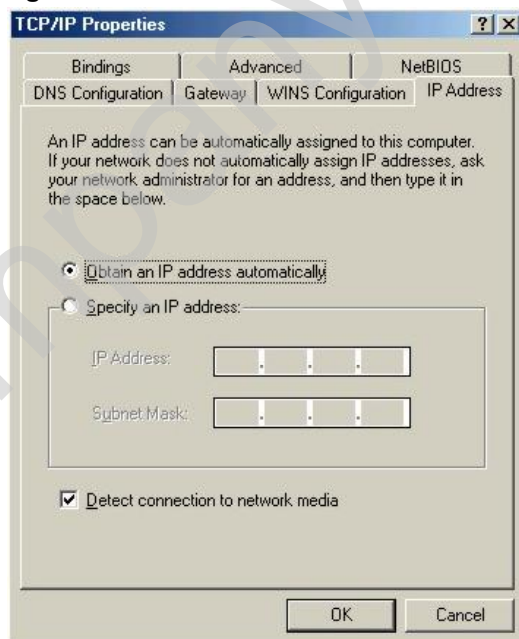
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

## Configuring

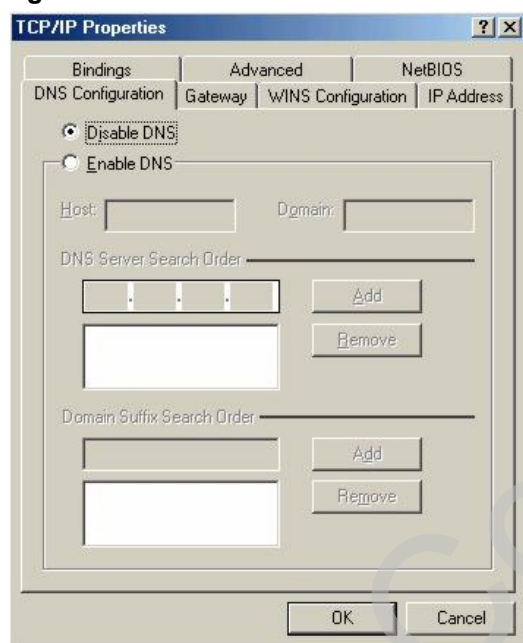
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 147** Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS** Configuration tab.
  - If you do not know your DNS information, select **Disable DNS**.
  - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 148** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



- 4 Click the **Gateway** tab.
  - If you do not know your gateway's IP address, remove previously installed gateways.
  - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Turn on your Prestige and restart your computer when prompted.

### Verifying Settings

- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

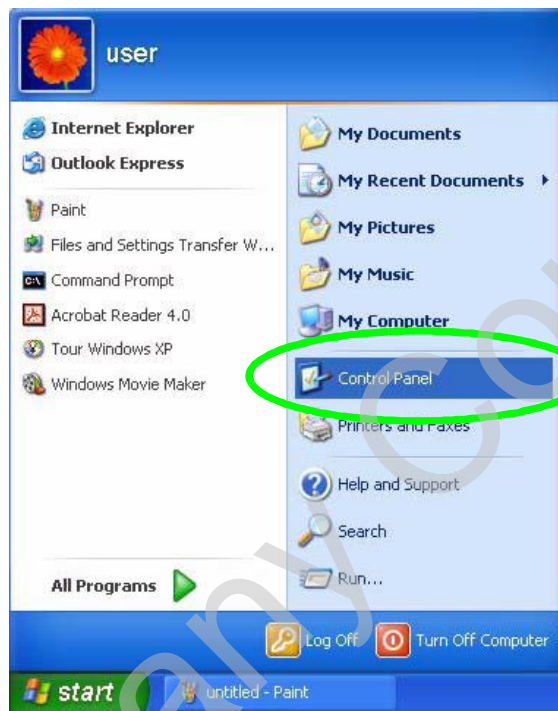
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

- 1 Click **start** (**Start** in Windows 2000/NT), **Settings, Control Panel**.

**Figure 149** Windows XP: Start Menu



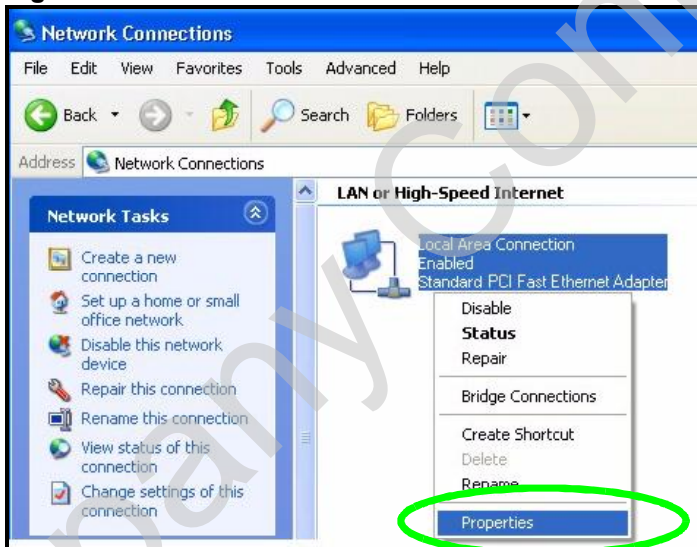
- 2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

**Figure 150** Windows XP: Control Panel



- 3 Right-click **Local Area Connection** and then click **Properties**.

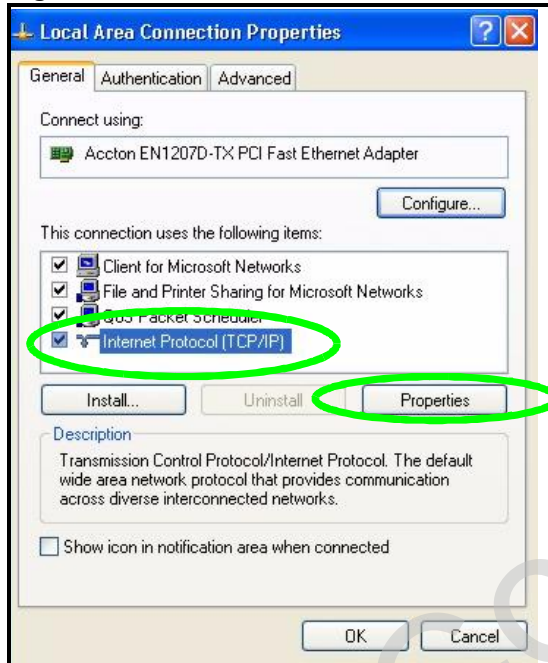
**Figure 151** Windows XP: Control Panel: Network Connections: Properties





- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

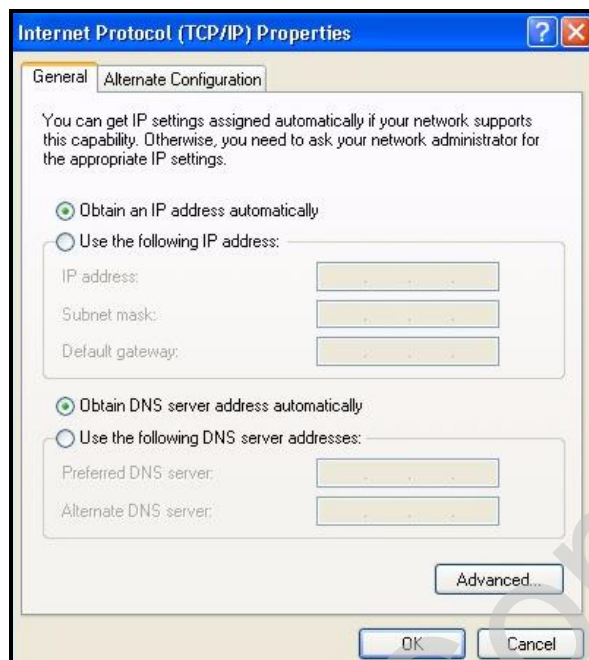
**Figure 152** Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).
  - If you have a dynamic IP address click **Obtain an IP address automatically**.
  - If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

**Figure 153** Windows XP: Internet Protocol (TCP/IP) Properties



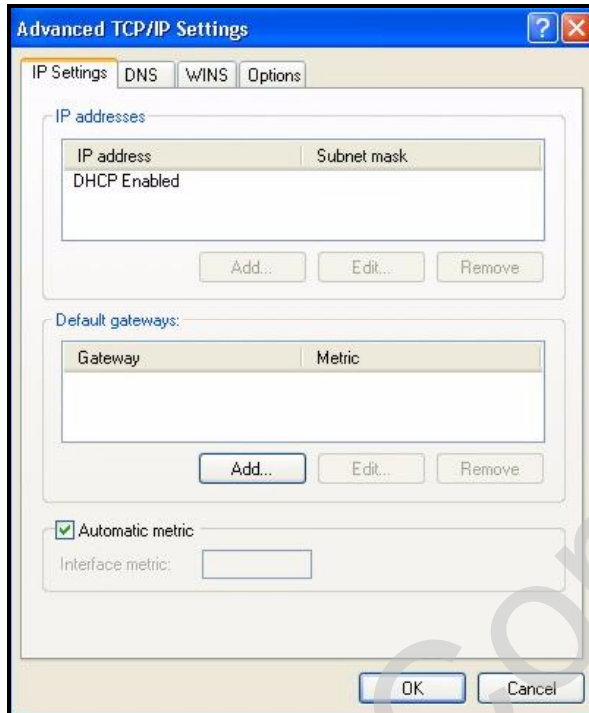
- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

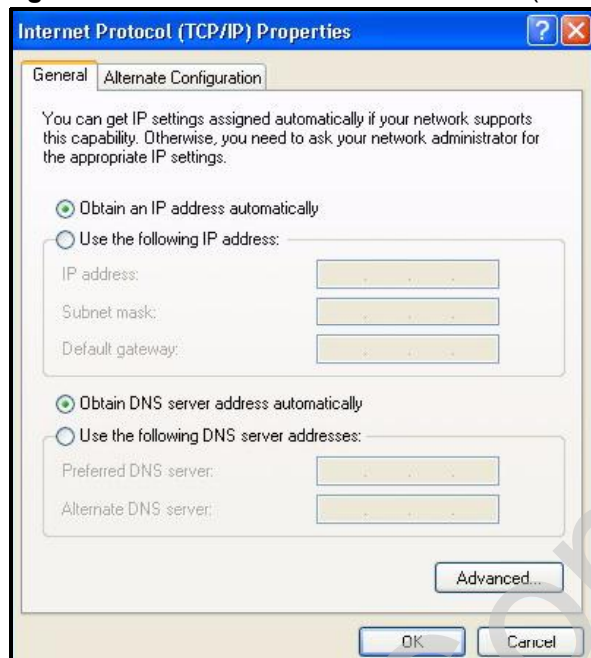
**Figure 154** Windows XP: Advanced TCP/IP Properties



- 7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):
  - Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
  - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 155** Windows XP: Internet Protocol (TCP/IP) Properties



- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **Close (OK)** in Windows 2000/NT to close the **Local Area Connection Properties** window.
- 10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11 Turn on your Prestige and restart your computer (if prompted).

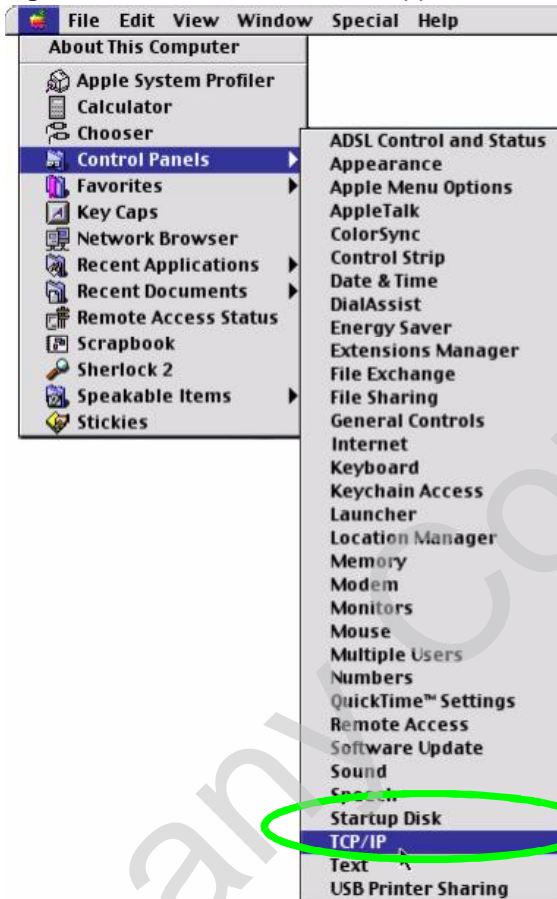
### Verifying Settings

- 1 Click **Start, All Programs, Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

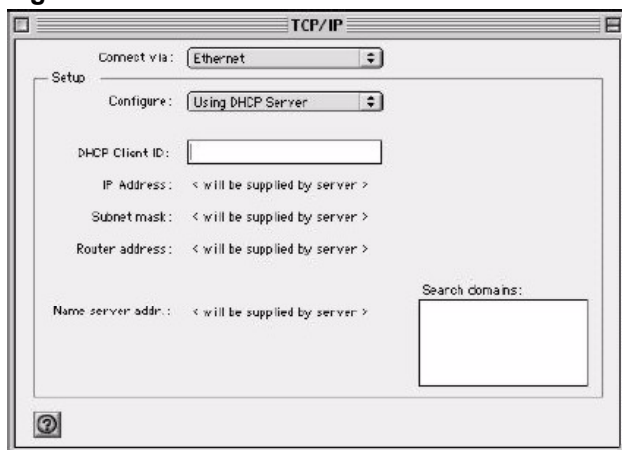
- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 156 Macintosh OS 8/9: Apple Menu



- 2 Select **Ethernet built-in** from the **Connect via** list.

**Figure 157** Macintosh OS 8/9: TCP/IP



- 3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your Prestige in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your Prestige and restart your computer (if prompted).

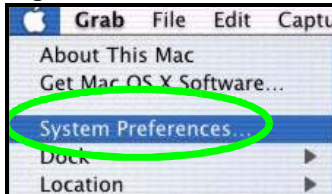
### Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

## Macintosh OS X

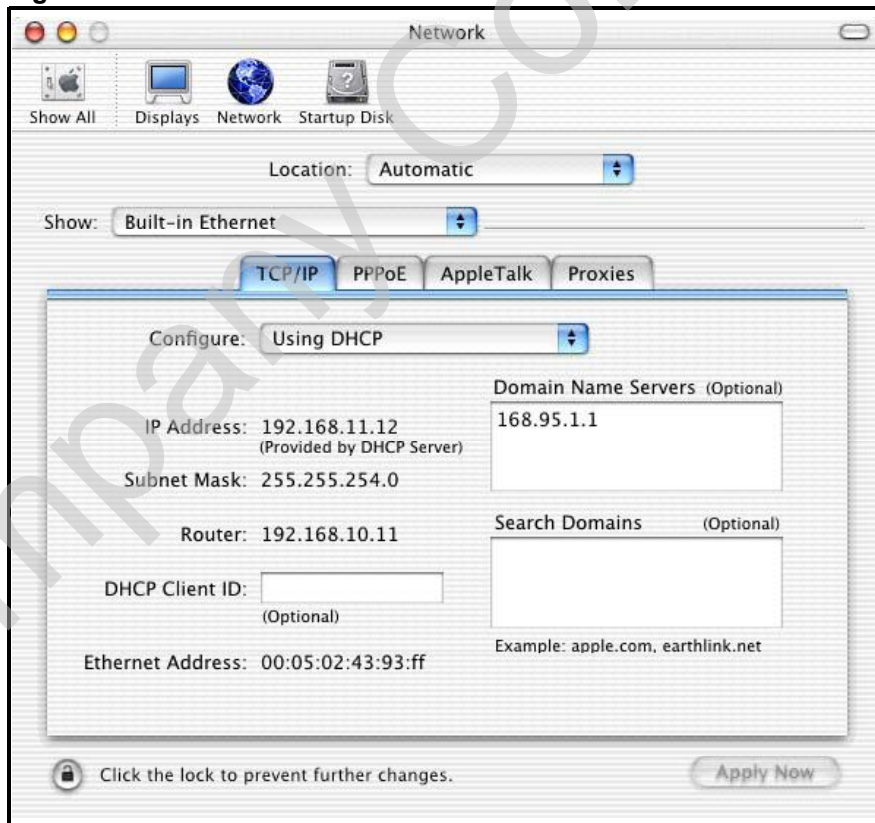
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 158** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 159** Macintosh OS X: Network



- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your Prestige in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your Prestige and restart your computer (if prompted).

### Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

Note: Make sure you are logged in as the root administrator.

### Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 160** Red Hat 9.0: KDE: Network Configuration: Devices





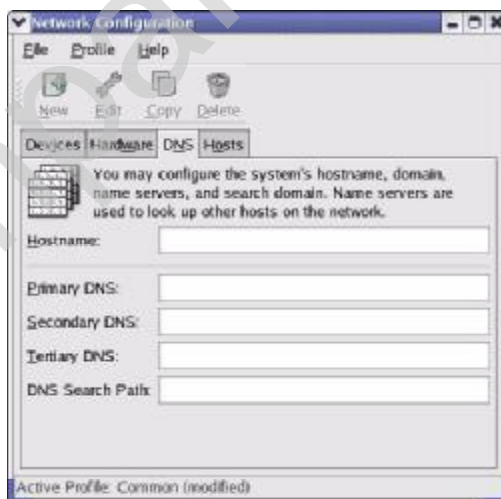
- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 161** Red Hat 9.0: KDE: Ethernet Device: General



- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
  - If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.
  - 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 162** Red Hat 9.0: KDE: Network Configuration: DNS



- 5 Click the **Devices** tab.
- 6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

**Figure 163** Red Hat 9.0: KDE: Network Configuration: Activate



- 7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

### Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
  - If you have a dynamic IP address, enter `dhcp` in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 164** Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 165** Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 166** Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 167** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:           [OK]
Shutting down loopback interface:       [OK]
Setting network parameters:             [OK]
Bringing up loopback interface:         [OK]
Bringing up interface eth0:             [OK]
```

### 32.1.1 Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 168** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

# Wireless LANs

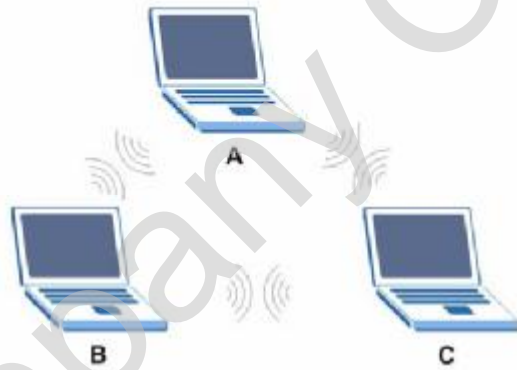
## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

**Figure 169** Peer-to-Peer Communication in an Ad-hoc Network



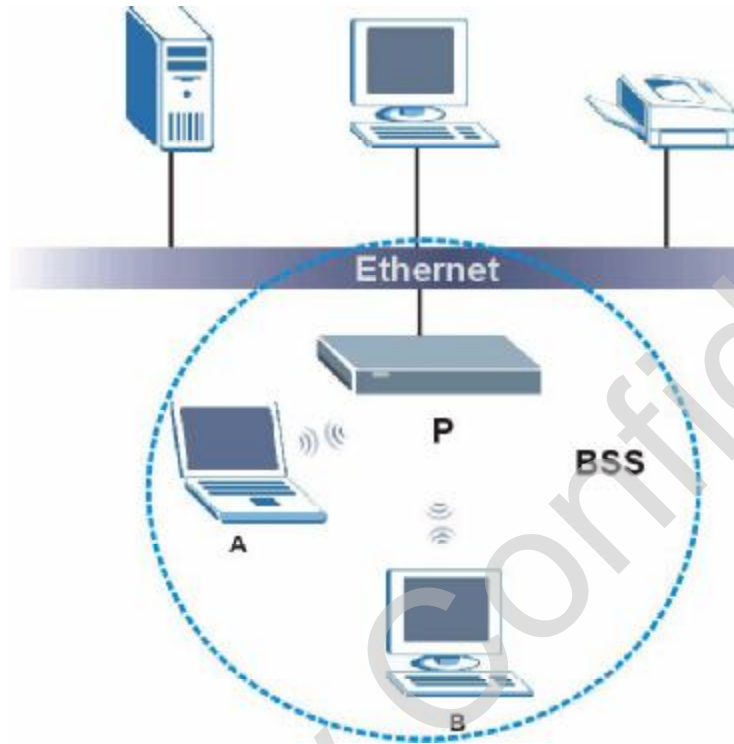
### BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

**Figure 170** Basic Service Set



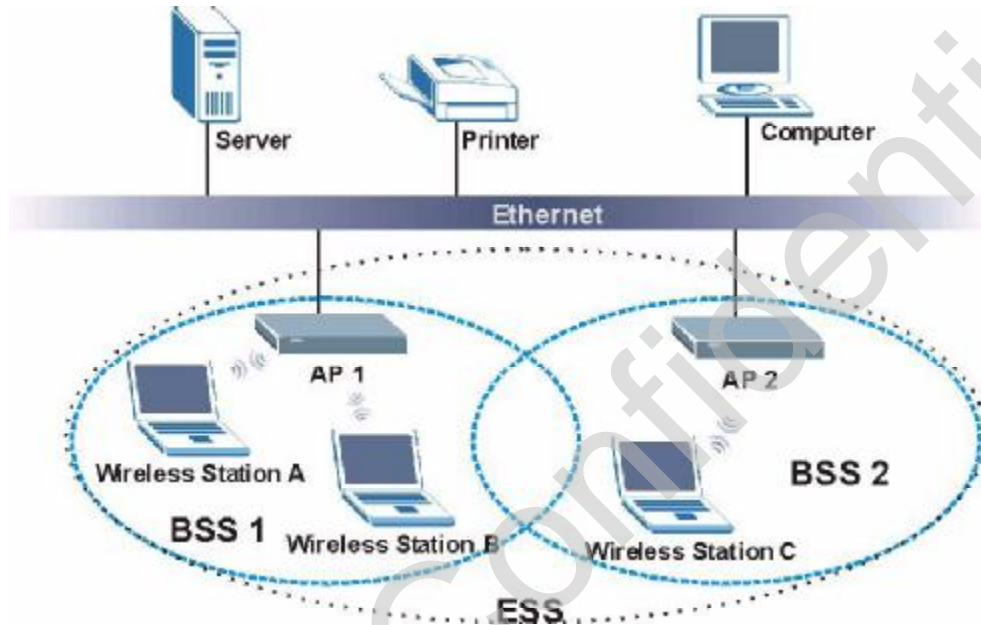
## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS Identification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

**Figure 171** Infrastructure WLAN



## Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

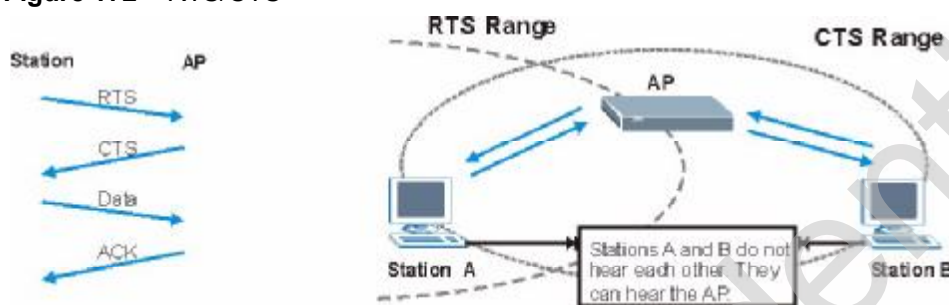
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 172** RTS/CTS



When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

**Note:** Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.



## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations MUST use the same preamble mode in order to communicate.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 92** IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication  
Determines the identity of the users.
- Authorization  
Determines the network services available to authenticated users once they are connected to the network.
- Accounting  
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

## Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**  
Sent by an access point requesting authentication.
- **Access-Reject**  
Sent by a RADIUS server rejecting access.
- **Access-Accept**  
Sent by a RADIUS server allowing access.
- **Access-Challenge**  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**  
Sent by the access point requesting accounting.
- **Accounting-Response**  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

## Types of Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

### EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### **EAP-TLS (Transport Layer Security)**

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### **EAP-TTLS (Tunneled Transport Layer Service)**

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

### **PEAP (Protected EAP)**

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

### **LEAP**

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

### **Dynamic WEP Key Exchange**

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with dynamic WEP key exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 93** Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

## WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

### Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

### **User Authentication**

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2 -PSK (WPA2 -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

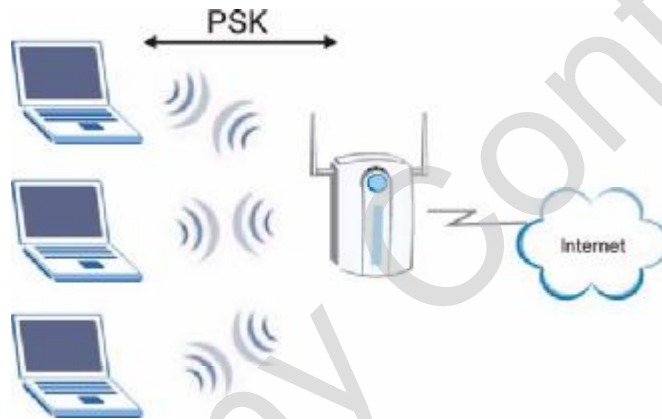
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

### 32.1.2 WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
- 3 The AP derives and distributes keys to the wireless clients.
- 4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

**Figure 173** WPA(2)-PSK Authentication



### 32.1.3 WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 94** Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable



## Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 95** Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.

**Table 95** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

**Table 95** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

**Table 95** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

# Legal Information

## Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

### Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause

harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.



#### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

#### 注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。減少電磁波影響，請妥適使用。

#### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### **Industry Canada Statement**

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- 1 this device may not cause interference and
- 2 this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

### **IMPORTANT NOTE:**

#### **IC Radiation Exposure Statement:**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

#### **Viewing Certifications**

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

## End-User License Agreement for "NBG-419N"

**WARNING:** ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.



## 1 Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

## 2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

## 3 Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

## 4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL on its Open Source web site (<ftp://opensource.zyxel.com>) (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand,

private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (<ftp://opensource.zyxel.com>), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

#### 5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

#### 6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

#### 7 Limitation of Liability

IN NO EVENT WILL ZyxEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyxEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyxEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

#### **8 Export Restrictions**

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyxEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

#### **9 Audit Rights**

ZyxEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

#### **10 Termination**

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyxEL all copies of the Software and Documentation in your possession or under your control. ZyxEL may terminate this License Agreement for any reason, including, but not limited to, if ZyxEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyxEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

## 11 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: NOTE: Some components of the Vantage CNM 2.3 incorporate source code covered under the Apache License, GPL License, LGPL License, Sun License, and Castor License. To obtain the source code covered under those Licenses, please check <ftp://opensource.zyxel.com> to get it.

# Index

## A

ActiveX [169](#)  
Address Assignment [120](#)  
Alert [199](#)  
alternative subnet mask notation [244](#)  
AP [21](#)  
AP (Access Point) [271](#)  
AP Mode  
    menu [76](#)  
    status screen [74, 81](#)  
AP+Bridge [21](#)  
Auto-bridge [132, 133](#)

## B

Bandwidth management  
    overview [173](#)  
    priority [176](#)  
    services [181](#)  
BitTorrent [181](#)  
Bridge/Repeater [21](#)  
bridged APs, security [102](#)  
BSS [269](#)

## C

CA [276](#)  
Certificate Authority [276](#)  
certifications [285](#)  
    notices [286](#)  
    viewing [287](#)  
Channel [65, 75, 271](#)  
    Interference [271](#)  
channel [100](#)  
Configuration  
    restore [208](#)

content filtering [167](#)  
    by keyword (in URL) [168](#)  
    by web feature [167](#)  
Cookies [169](#)  
copyright [285](#)  
CPU usage [66, 75, 83](#)  
CTS (Clear to Send) [272](#)

## D

Daylight saving [202](#)  
DDNS [151](#)  
    see also Dynamic DNS  
    service providers [152](#)  
DHCP [44, 139](#)  
    DHCP server  
    see also Dynamic Host Configuration Protocol  
DHCP server [136, 139](#)  
DHCP table [44](#)  
    DHCP client information  
    DHCP status  
Dimensions [225](#)  
disclaimer [285](#)  
DNS [141](#)  
DNS Server [120](#)  
DNS server [141](#)  
Domain Name System [141](#)  
Domain Name System. See DNS.  
duplex setting [66, 76, 83](#)  
Dynamic DNS [151](#)  
Dynamic Host Configuration Protocol [139](#)  
Dynamic WEP Key Exchange [276](#)  
DynDNS [152](#)  
DynDNS see also DDNS [152](#)

**E**

EAP Authentication [275](#)  
Encryption [277](#)  
encryption [101](#)  
    key [102](#)  
    WPA compatible [102](#)  
ESS [270](#)  
ESSID [222](#)  
Extended Service Set [270](#)

**F**

FCC interference statement [285](#)  
File Transfer Program [181](#)  
Firewall  
    ICMP packets [163](#)  
Firmware upload [205](#)  
    file extension  
    using HTTP  
firmware version [65](#), [74](#), [82](#)  
Fragmentation Threshold [273](#)  
FTP. see also File Transfer Program [181](#)

**G**

General wireless LAN screen [103](#)

**H**

Hidden Node [271](#)  
HTTP [181](#)  
Hyper Text Transfer Protocol [181](#)

**I**

IANA [250](#)  
IBSS [269](#)  
IEEE 802.11g [273](#)

IGMP [121](#)

    see also Internet Group Multicast Protocol version

IGMP version [121](#)

Independent Basic Service Set [269](#)

Internet Assigned Numbers Authority  
    See IANA

Internet Group Multicast Protocol [121](#)

IP Address [137](#), [138](#), [144](#), [145](#)

IP alias [137](#)

IP Pool [140](#)

**J**

Java [169](#)

**L**

LAN [135](#)

    IP pool setup [136](#)

LAN overview [135](#)

LAN setup [135](#)

LAN TCP/IP [136](#)

Language [211](#)

Link type [66](#), [75](#), [83](#)

Local Area Network [135](#)

Log [200](#)

**M**

MAC [109](#)

MAC address [101](#), [121](#)  
    cloning [121](#)

MAC address filter [101](#)

MAC address filtering [109](#)

MAC filter [109](#)

managing the device

    good habits [22](#)

    using the web configurator. See web configurator.

    using the wireless switch.

using the WPS. See WPS.

MBSSID [21](#)

Media access control [109](#)

Memory usage [66](#), [75](#), [83](#)

mode [21](#)

Multicast [121](#)

IGMP [121](#)

## N

NAT [143](#), [144](#), [249](#)

how it works [143](#)

overview [143](#)

see also Network Address Translation

NAT Traversal [187](#)

Navigation Panel [67](#), [76](#)

navigation panel [67](#), [76](#)

Network Address Translation [143](#), [144](#)

## O

Operating Channel [65](#), [75](#)

operating mode [21](#)

## P

P2P [181](#)

peer-to-peer [181](#)

Point-to-Point Protocol over Ethernet [124](#)

Point-to-Point Tunneling Protocol [126](#)

Pool Size [140](#)

Port forwarding [145](#)

default server [145](#)

local server [145](#)

port speed [66](#), [76](#), [83](#)

Power Specification [225](#)

PPPoE [124](#)

dial-up connection

PPTP [126](#)

Preamble Mode [273](#)

product registration [288](#)

## Q

Quality of Service (QoS) [111](#)

## R

RADIUS [274](#)

Shared Secret Key [275](#)

RADIUS Message Types [275](#)

RADIUS Messages [275](#)

registration

product [288](#)

related documentation [3](#)

Remote management

and NAT [184](#)

limitations [183](#)

system timeout [184](#)

Reset button [41](#)

Reset the device [41](#)

Restore configuration [208](#)

RF (Radio Frequency) [226](#)

RIP [157](#)

Roaming [110](#)

RTS (Request To Send) [272](#)

RTS Threshold [271](#), [272](#)

RTS/CTS Threshold [100](#), [110](#)

## S

safety warnings [7](#)

Scheduling [114](#)

Security Parameters [280](#)

Service and port numbers [165](#), [180](#)

Service Set [59](#), [103](#)

Service Set IDentification [59](#), [103](#)

Service Set IDentity. See SSID.

Session Initiated Protocol [181](#)

SIP [181](#)

SSID [59](#), [65](#), [75](#), [82](#), [100](#), [103](#)

Static DHCP [140](#)

Static Route [153](#)

Status [64](#)

- subnet [241](#)
- Subnet Mask [137](#), [138](#)
- subnet mask [242](#)
- subnetting [245](#)
- Summary
  - DHCP table [44](#)
  - Packet statistics [45](#)
  - Wireless station status [46](#)
- syntax conventions [5](#)
- Sys Op Mode [213](#)
- System General Setup [197](#)
- System Name [198](#)
- System restart [211](#)

## T

- TCP/IP configuration [139](#)
- Temperature [225](#)
- Time setting [201](#)
- trigger port [147](#)
- Trigger port forwarding [147](#)
  - example [149](#)
  - process [149](#)

## U

- Universal Plug and Play [187](#)
  - Application [188](#)
  - Security issues [188](#)
- UPnP [187](#)
- URL Keyword Blocking [169](#)
- Use Authentication [278](#)
- User Name [152](#)

## V

- VoIP [181](#)
- VPN [126](#)

## W

- WAN (Wide Area Network) [119](#)
- WAN advanced [132](#)
- WAN MAC address [121](#)
- warranty [288](#)
  - note [288](#)
- Web Configurator
  - how to access [37](#)
  - Overview [37](#)
- web configurator [22](#)
- Web Proxy [169](#)
- WEP Encryption [86](#), [106](#), [108](#)
- WEP encryption [105](#)
- WEP key [105](#)
- Wireless association list [46](#)
- wireless channel [222](#)
- wireless LAN [222](#)
- wireless LAN scheduling [114](#)
- Wireless network
  - basic guidelines [100](#)
  - channel [100](#)
  - encryption [101](#)
  - example [99](#)
  - MAC address filter [101](#)
  - overview [99](#)
  - security [100](#)
  - SSID [100](#)
- Wireless security [100](#)
  - overview [100](#)
  - type [100](#)
- wireless security [222](#)
- wireless switch [22](#)
- Wireless tutorial [89](#)
  - WPS [89](#)
- Wizard setup [25](#)
- WLAN
  - Interference [271](#)
  - Security Parameters [280](#)
- World Wide Web [181](#)
- WPA compatible [102](#)
- WPA, WPA2 [277](#)
- WPS [22](#)
- WWW [181](#)



**X**

Xbox Live [181](#)

Company Confidential

Company Confidential