

NBG-417N

Wireless N-lite Home Router

User's Guide

Default Login Details

IP Address	http://192.168.1.1
Password	1234



Firmware Version 1.0
Edition 1, 1/2009

www.zyxel.com

ZyXEL

Copyright © 2009
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NBG-417N 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 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

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 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.










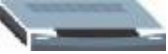
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NBG-417N may be referred to as the "NBG-417N", 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-417N icon is not an exact representation of your device.

NBG-417N 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 
Modem 		

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.



Contents Overview

Introduction	19
Getting to Know Your NBG-417N	21
The WPS Button	25
Introducing the Web Configurator	27
Connection Wizard	39
AP Mode	53
Tutorials	61
Network	69
Wireless LAN	71
WAN	91
LAN	103
DHCP Server	107
Network Address Translation (NAT)	113
Dynamic DNS	123
Security	127
Firewall	129
Content Filtering	135
Management	141
Static Route	143
Bandwidth Management	147
Remote Management	155
Universal Plug-and-Play (UPnP)	159
Maintenance and Troubleshooting	173
System	175
Logs	181
Tools	183
Sys OP Mode	189
Language	193
Troubleshooting	195
Appendices and Index	203

Table of Contents

About This User's Guide	3
Document Conventions	5
Safety Warnings	7
Contents Overview	9
Table of Contents	11
Part I: Introduction	19
Chapter 1	
Getting to Know Your NBG-417N	21
1.1 Overview	21
1.2 Applications	21
1.3 Ways to Manage the NBG-417N	22
1.4 Good Habits for Managing the NBG-417N	22
1.5 LEDs	22
Chapter 2	
The WPS Button	25
2.1 Overview	25
Chapter 3	
Introducing the Web Configurator	27
3.1 Web Configurator Overview	27
3.2 Accessing the Web Configurator	27
3.3 Resetting the NBG-417N	29
3.3.1 Procedure to Use the Reset Button	29
3.4 Navigating the Web Configurator	29
3.5 The Status Screen in Router Mode	30
3.5.1 Navigation Panel	32
3.5.2 Summary: DHCP Table	34
3.5.3 Summary: Packet Statistics	35
3.5.4 Summary: WLAN Station Status	36
Chapter 4	
Connection Wizard	39

4.1 Wizard Setup	39
4.2 Connection Wizard: STEP 1: System Information	40
4.2.1 System Name	40
4.2.2 Domain Name	41
4.3 Connection Wizard: STEP 2: Wireless LAN	42
4.3.1 Extend (WPA-PSK or WPA2-PSK) Security	43
4.4 Connection Wizard: STEP 3: Internet Configuration	43
4.4.1 Ethernet Connection	44
4.4.2 PPPoE Connection	44
4.4.3 PPTP Connection	46
4.4.4 Your IP Address	47
4.4.5 WAN IP Address Assignment	48
4.4.6 IP Address and Subnet Mask	48
4.4.7 DNS Server Address Assignment	49
4.4.8 WAN IP and DNS Server Address Assignment	50
4.4.9 WAN MAC Address	51
4.5 Connection Wizard Complete	52
Chapter 5	
AP Mode.....	53
5.1 AP Mode Overview	53
5.2 Setting your NBG-417N to AP Mode	53
5.3 The Status Screen in AP Mode	54
5.3.1 Navigation Panel	56
5.4 Configuring Your Settings	57
5.4.1 LAN Settings	57
5.4.2 WLAN and Maintenance Settings	58
5.5 Logging in to the Web Configurator in AP Mode	58
Chapter 6	
Tutorials.....	61
6.1 How to Connect to the Internet from an AP	61
6.2 Configure Wireless Security Using WPS on both your NBG-417N and Wireless Client	61
6.2.1 Push Button Configuration (PBC)	62
6.2.2 PIN Configuration	63
6.3 Enable and Configure Wireless Security without WPS on your NBG-417N	65
6.4 Configure Your Notebook	66
Part II: Network.....	69
Chapter 7	
Wireless LAN.....	71

7.1 Overview	71
7.2 What You Can Do In the Wireless LAN Screen	72
7.3 What You Should Know About Wireless LAN	72
7.3.1 Wireless Security Overview	72
7.4 General Wireless LAN Screen	75
7.4.1 No Security	76
7.4.2 WEP Encryption	77
7.4.3 WPA-PSK/WPA2-PSK	79
7.5 MAC Filter	80
7.6 Wireless LAN Advanced Screen	82
7.7 Quality of Service (QoS) Screen	83
7.7.1 Application Priority Configuration	85
7.8 WPS Screen	87
7.9 WPS Station Screen	88
7.10 Scheduling Screen	88
Chapter 8	
WAN.....	91
8.1 Overview	91
8.2 What You Can Do In the WAN Screens	91
8.3 What You Need To Know About WAN	92
8.3.1 Configuring Your Internet Connection	92
8.3.2 Multicast	93
8.3.3 NetBIOS over TCP/IP	94
8.3.4 Auto-Bridge	94
8.4 Internet Connection	95
8.4.1 Ethernet Encapsulation	95
8.4.2 PPPoE Encapsulation	96
8.4.3 PPTP Encapsulation	98
8.5 Advanced WAN Screen	101
Chapter 9	
LAN.....	103
9.1 Overview	103
9.2 What You Can Do in the LAN Screen	103
9.3 What You Need To Know About LAN	104
9.3.1 IP Pool Setup	104
9.3.2 LAN TCP/IP	104
9.4 LAN IP Screen	105
Chapter 10	
DHCP Server.....	107
10.1 Overview	107

10.2 What You Can Do in the DHCP Server Screens	107
10.3 What You Need To Know About the DHCP Server Screens	107
10.4 General Screen	108
10.5 Advanced Screen	108
10.6 Client List Screen	110
Chapter 11	
Network Address Translation (NAT).....	113
11.1 Overview	113
11.2 What You Can Do in the NAT Screens	114
11.3 What You Need To Know About NAT	114
11.3.1 What NAT Does	115
11.3.2 How NAT Works	115
11.4 General NAT Screen	116
11.5 NAT Application Screen	117
11.6 NAT Advanced Screen	119
11.7 Technical Reference	120
11.8 Using NATPort Forwarding: Services and Port Numbers	120
11.8.1 Configuring Servers Behind Port Forwarding Example	120
11.9 Trigger Port Forwarding	121
11.9.1 Trigger Port Forwarding Example	122
11.9.2 Two Points To Remember About Trigger Ports	122
Chapter 12	
Dynamic DNS	123
12.1 Overview	123
12.2 What You Can Do in the DDNS Screen	123
12.3 What You Need To Know About DDNS	123
12.3.1 DynDNS Wildcard	123
12.4 Dynamic DNS Screen	124
Part III: Security.....	127
Chapter 13	
Firewall.....	129
13.1 Overview	129
13.2 What You Can Do in the Firewall Screens	129
13.3 What You Need To Know About Firewall	130
13.3.1 What is a Firewall?	130
13.3.2 Stateful Inspection Firewall	130
13.3.3 About the NBG-417N Firewall	130

13.3.4 Guidelines For Enhancing Security With Your Firewall	131
13.4 General Firewall Screen	132
13.5 Services Screen	132
Chapter 14	
Content Filtering	135
14.1 Overview	135
14.2 What You Can Do in the Content Filtering Screen	135
14.3 What You Need To Know About Content Filtering	135
14.3.1 Content Filtering Profiles	135
14.4 Filter Screen	137
14.5 Technical Reference	138
14.5.1 Customizing Keyword Blocking URL Checking	138
Part IV: Management.....	141
Chapter 15	
Static Route	143
15.1 Overview	143
15.2 What You Can Do in the IP Static Route Screens	144
15.3 IP Static Route Screen	144
15.3.1 Static Route Setup Screen	145
Chapter 16	
Bandwidth Management.....	147
16.1 Overview	147
16.2 What You Can Do in the Bandwidth Management Screen	147
16.3 What You Need To Know About Bandwidth Management	148
16.4 Bandwidth Management General Configuration	148
16.5 Bandwidth Management Advanced Configuration	150
16.5.1 Rule Configuration: User Defined Service Rule Configuration	152
16.6 Technical References	153
16.6.1 Application and Subnet-based Bandwidth Management	153
16.6.2 Bandwidth Management Priorities	153
16.6.3 Predefined Bandwidth Management Services	154
16.6.4 Services and Port Numbers	154
Chapter 17	
Remote Management.....	155
17.1 Overview	155
17.2 What You Can Do in the Remote Management Screens	155

17.3 What You Need To Know About Remote Management	155
17.3.1 Remote Management Limitations	155
17.3.2 Remote Management and NAT	156
17.3.3 System Timeout	156
17.4 WWW Screen	157
Chapter 18	
Universal Plug-and-Play (UPnP).....	159
18.1 Overview	159
18.2 What You Can Do in the UPnP Screen	159
18.3 What You Need to Know About UPnP	159
18.4 UPnP Screen	161
18.5 Technical Reference	161
18.5.1 Installing UPnP in Windows Example	162
Part V: Maintenance and Troubleshooting	173
Chapter 19	
System	175
19.1 Overview	175
19.2 What You Can Do in the System Screens	175
19.3 System General Screen	175
19.4 Time Setting Screen	177
Chapter 20	
Logs	181
20.1 Overview	181
20.2 What You Can Do in the Log Screens	181
20.3 What You Need to Know About Logs	181
20.4 View Log Screen	182
Chapter 21	
Tools.....	183
21.1 Overview	183
21.2 What You Can Do in the Tools Screen	183
21.3 Firmware Upload Screen	183
21.4 Configuration Screen	186
21.4.1 Backup Configuration	186
21.4.2 Restore Configuration	187
21.4.3 Back to Factory Defaults	188
21.5 Restart Screen	188

Chapter 22	
Sys OP Mode	189
22.1 Overview	189
22.2 What You Can Do in the Sys OP Mode Screen	189
22.3 What You Need to Know About Sys OP Mode	190
22.4 General Screen	191
Chapter 23	
Language	193
23.1 Language Screen	193
Chapter 24	
Troubleshooting	195
24.1 Power, Hardware Connections, and LEDs	195
24.2 NBG-417N Access and Login	196
24.3 Internet Access	198
24.4 Resetting the NBG-417N to Its Factory Defaults	200
24.5 Wireless Router/AP Troubleshooting	200
Part VI: Appendices and Index	203
Appendix A Product Specifications.....	205
Appendix B Pop-up Windows, JavaScripts and Java Permissions	209
Appendix C IP Addresses and Subnetting	217
Appendix D Setting up Your Computer's IP Address	227
24.5.1 Verifying Settings	244
Appendix E Wireless LANs	245
24.5.2 WPA(2)-PSK Application Example	255
24.5.3 WPA(2) with RADIUS Application Example	255
Appendix F Services	257
Appendix G Legal Information.....	261
Index	265

PART I

Introduction

Getting to Know Your NBG-417N (21)

The WPS Button (25)

Introducing the Web Configurator (27)

Connection Wizard (39)

AP Mode (53)

Tutorials (61)

Getting to Know Your NBG-417N

1.1 Overview

This chapter introduces the main features and applications of the NBG-417N.

The NBG-417N 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-417N:

- **Wired.** You can connect network devices via the Ethernet ports of the NBG-417N so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the NBG-417N to access network resources.
- **WAN.** Connect to a broadband modem/router for Internet access.

Figure 1 NBG-417N Network



1.3 Ways to Manage the NBG-417N

Use any of the following methods to manage the NBG-417N.

- WPS (Wi-Fi Protected Setup). You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL Device.
- Web Configurator. This is recommended for everyday management of the NBG-417N using a (supported) web browser.

1.4 Good Habits for Managing the NBG-417N

Do the following things regularly to make the NBG-417N more secure and to manage the NBG-417N 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-417N to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG-417N. 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-417N is receiving power and functioning properly.
		Off	The NBG-417N is not receiving power.
WLAN / WPS 	Green	On	The NBG-417N is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG-417N is sending/receiving data through the wireless LAN. The NBG-417N is negotiating a WPS connection with a wireless client.
		Off	The wireless LAN is not ready or has failed.
WAN 	Green	On	The NBG-417N has a successful 10/100MB WAN connection.
		Blinking	The NBG-417N is sending/receiving data through the WAN.
		Off	The WAN connection is not ready, or has failed.
LAN 1-4 	Green	On	The NBG-417N has a successful 10/100MB Ethernet connection.
		Blinking	The NBG-417N is sending/receiving data through the LAN.
		Off	The LAN is not connected.
WPS Button 	Press this button for 1 second to set up a wireless connection via WiFi Protected Setup with another WPS-enabled client. You must press the WPS button on the client side within 120 seconds for a successful connection.		

The WPS Button

2.1 Overview

Your NBG-417N supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

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

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

For more information on using WPS, see [Section 6.2 on page 61](#).

Introducing the Web Configurator

This chapter describes how to access the NBG-417N Web Configurator and provides an overview of its screens.

3.1 Web Configurator Overview

The Web Configurator is an HTML-based management interface that allows easy setup and management of the NBG-417N via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions or Safari 2.0 or later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

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

3.2 Accessing the Web Configurator

- 1 Make sure your NBG-417N hardware is properly connected and prepare your computer or computer network to connect to the NBG-417N (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.

- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 3 Change Password Screen



Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the NBG-417N if this happens.

- 6 Select the setup mode you want to use.
 - Click **Go to Wizard Setup** to use the Configuration Wizard for basic Internet and Wireless setup.
 - Click **Go to Advanced Setup** to view and configure all the NBG-417N's settings.

- Select a language to go to the basic Web Configurator in that language. To change to the advanced configurator see [Chapter 23 on page 193](#).

Figure 4 Selecting the setup mode



3.3 Resetting the NBG-417N

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-417N 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-417N.
- 3 Press the **RESET** button for longer than five seconds to set the NBG-417N back to its factory-default configurations.

3.4 Navigating the Web Configurator

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

3.5 The Status Screen in Router Mode

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






(For information on the status screen in **AP Mode** see [Chapter 5 on page 54.](#))

Figure 5 Web Configurator Status Screen



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

Table 2 Status Screen Icon Key

ICON	DESCRIPTION
	Click this icon to open the setup wizard.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the Web Configurator.
	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.

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

Table 3 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the System Name you enter in the Maintenance > System > General screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- DHCP	This shows the WAN port's DHCP role - Client or None .
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - Server or None .
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - On , Off or Off by scheduler .
- Name (SSID)	This shows a descriptive name used to identify the NBG-417N in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG-417N is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG-417N is using.
- 802.11 Mode	This shows the wireless standard.
- WPS	This displays Configured when the WPS has been set up. This displays Unconfigured if the WPS has not been set up. Click the status to display Network > Wireless LAN > WPS screen.
System Status	
System Up Time	This is the total time the NBG-417N has been on.
Current Date/Time	This field displays your NBG-417N's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG-417N's processing ability is currently used. When this percentage is close to 100%, the NBG-417N 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).

Table 3 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
- Memory Usage	This shows what percentage of the heap memory the NBG-417N is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall.
System Setting	
- Firewall	This shows whether the firewall is active or not.
- Bandwidth Management	This shows whether the bandwidth management is active or not.
- UPnP	This shows whether UPnP is active or not.
Interface Status	
Interface	This displays the NBG-417N port types. The port types are: WAN , LAN and WLAN .
Status	For the LAN and WAN ports, this field displays Down (line is down) or Up (line is up or connected). For the WLAN, it displays Up when the WLAN is enabled or Down when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or N/A when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays N/A when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled.
Summary	
DHCP Table	Use this screen to view current DHCP client information.
Packet Statistics	Use this screen to view port status and packet specific statistics.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the NBG-417N.

3.5.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG-417N features.

The following table describes the sub-menus.

Table 4 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG-417N's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		

Table 4 Screens Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG-417N to block access to devices or block the devices from accessing the NBG-417N.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	Advanced	Use this screen to configure other advanced properties.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
DHCP Server	General	Use this screen to enable the NBG-417N's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the NBG-417N.
	Advanced	Use this screen to change your NBG-417N's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Filter	Use this screen to block certain web features and sites containing certain keywords in the URL.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes.

Table 4 Screens Summary

LINK	TAB	FUNCTION
Bandwidth MGMT	General	Use this screen to enable bandwidth management.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG-417N.
UPnP	General	Use this screen to enable UPnP on the NBG-417N.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG-417N's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your NBG-417N.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG-417N.
	Restart	This screen allows you to reboot the NBG-417N without turning the power off.
Sys OP Mode	General	This screen allows you to select whether your device acts as a Router or a Access Point.
Language		This screen allows you to select the language you prefer.

3.5.2 Summary: 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-417N's LAN as a DHCP server or disable it. When configured as a server, the NBG-417N 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-417N's DHCP server.

Figure 6 Summary: DHCP Table

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

Refresh

The following table describes the labels in this screen.

Table 5 Summary: DHCP Table

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

3.5.3 Summary: Packet Statistics

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

Figure 7 Summary: Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx U/s	Rx U/s
WAN	UP	374735	370218	0	0	157
LAN	UP	310750	365932	0	321	1575
WLAN	UP	255	2117	0	0	0

System Up Time : 1:41:47

Poll Interval : 5 sec Refresh Refresh

The following table describes the labels in this screen.

Table 6 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG-417N's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or Down when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays Down when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and Down when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
System Up Time	This is the total time the NBG-417N has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval(s) field.
Stop	Click Stop to stop refreshing statistics.

3.5.4 Summary: 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-417N 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 8 Summary: Wireless Association List



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

Refresh

The following table describes the labels in this screen.

Table 7 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the NBG-417N's WLAN network.
Refresh	Click Refresh to reload the list.

4

Connection Wizard

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

4.1 Wizard Setup

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

- 1 After you access the NBG-417N Web Configurator, click the **Go to Wizard setup** hyperlink.

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

Figure 9 Select Wizard or Advanced Mode



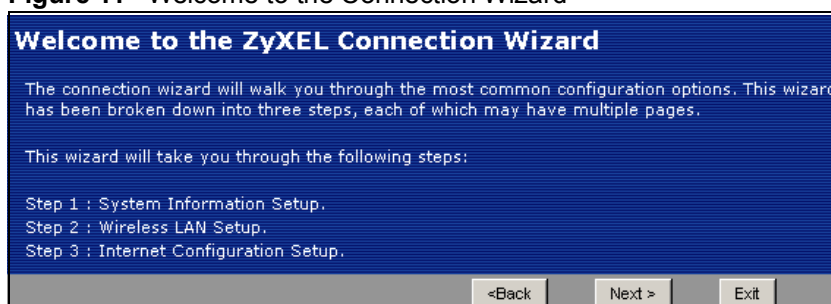
- 2 Choose a language by clicking on the language's button. The screen will update. Click the **Next** button to proceed to the next screen.

Figure 10 Select a Language



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

Figure 11 Welcome to the Connection Wizard



4.2 Connection Wizard: STEP 1: System Information

System Information contains administrative and system-related information.

4.2.1 System Name

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

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start, Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.

- In Windows XP, click **Start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the NBG-417N **System Name**.

4.2.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the NBG-417N via DHCP.

Click **Next** to configure the NBG-417N for Internet access.

Figure 12 Wizard Step 1: System Information

The screenshot shows a wizard window titled 'STEP 1' with a blue background. At the top, it says 'System Information'. Under the heading 'System Name', there is a text box containing 'NBG-417N'. Below that, under the heading 'Domain Name', there is a text box containing 'zyxel.com'. At the bottom right, there are three buttons: '<Back', 'Next >', and 'Exit'.

The following table describes the labels in this screen.

Table 8 Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG-417N in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

4.3 Connection Wizard: STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

Figure 13 Wizard Step 2: Wireless LAN

The following table describes the labels in this screen.

Table 9 Wizard Step 2: Wireless LAN

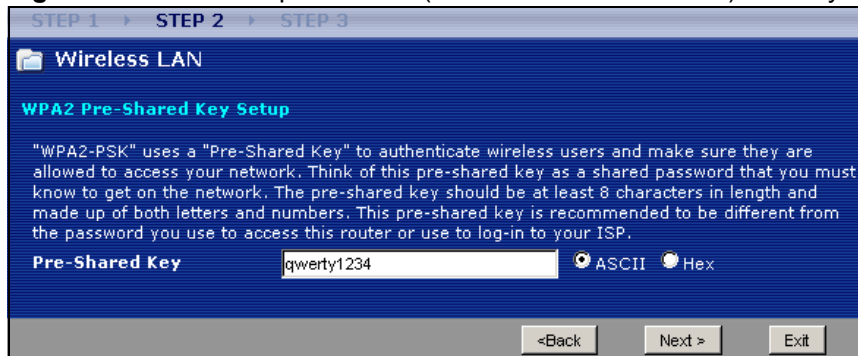
LABEL	DESCRIPTION
Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG-417N, make sure all wireless stations use the same SSID in order to access the network.
Security	Select a Security level from the drop-down list box. Choose Auto (WPA2-PSK) to have the NBG-417N generate a pre-shared key automatically. After you click Next a screen pops up displaying the generated pre-shared key. Write down the key for use later when connecting other wireless devices to your network. Click OK to continue. Choose None to have no wireless LAN security configured. If you do not enable any wireless security on your NBG-417N, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to Section 4.4 on page 43 . Choose Extend (WPA-PSK or WPA2-PSK) security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK or WPA2-PSK respectively. If you choose this option, skip directly to Section 4.3.1 on page 43 .
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. The device will automatically select the channel with the least interference.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen.
Exit	Click Exit to close the wizard screen without saving.

Note: The wireless stations and NBG-417N must use the same SSID, channel ID, WPA-PSK (if WPA-PSK is enabled) or WPA2-PSK (if WPA2-PSK is enabled) for wireless communication.

4.3.1 Extend (WPA-PSK or WPA2-PSK) Security

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

Figure 14 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security



The following table describes the labels in this screen.

Table 10 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

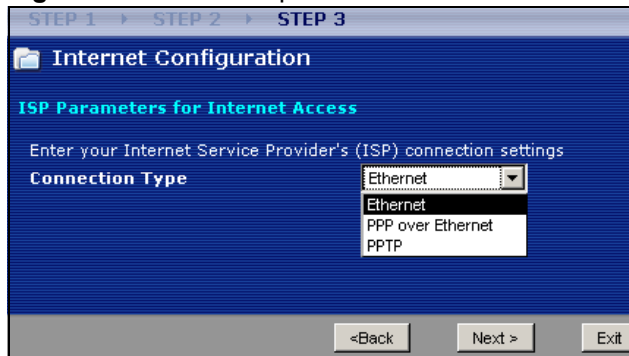
LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII or HEX characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click Back to display the previous screen.
Next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

4.4 Connection Wizard: STEP 3: Internet Configuration

The NBG-417N offers three Internet connection types. They are **Ethernet**, **PPP over Ethernet** or **PPTP**. The wizard attempts to detect which WAN connection type you are using. If the wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

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

Figure 15 Wizard Step 3: ISP Parameters.



The following table describes the labels in this screen,

Table 11 Wizard Step 3: ISP Parameters

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

4.4.1 Ethernet Connection

Choose **Ethernet** when the WAN port is used as a regular Ethernet. Continue to [Section 4.4.4 on page 47](#).

Figure 16 Wizard Step 3: Ethernet Connection



4.4.2 PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host

personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

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

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

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/ carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the NBG-417N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG-417N does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.

Figure 17 Wizard Step 3: PPPoE Connection

The following table describes the labels in this screen.

Table 12 Wizard Step 3: PPPoE Connection

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

4.4.3 PPTP Connection

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

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

Refer to the appendix for more information on PPTP.

Note: The NBG-417N supports one PPTP server connection at any given time.

Figure 18 Wizard Step 3: PPTP Connection

The following table describes the fields in this screen

Table 13 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select PPTP from the drop-down list box. To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
Server IP Address	Type the IP address of the PPTP server.

Table 13 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this radio button, provided by your ISP to give the NBG-417N a fixed, unique IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

4.4.4 Your IP Address

The following wizard screen allows you to assign a fixed IP address or give the NBG-417N an automatically assigned IP address depending on your ISP.

Figure 19 Wizard Step 3: Your IP Address

The following table describes the labels in this screen

Table 14 Wizard Step 3: Your IP Address

LABEL	DESCRIPTION
Get automatically from your ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection. If you choose this option, skip directly to Section 4.4.9 on page 51 .
Use fixed IP address provided by your ISP	Select this option if you were given IP address and/or DNS server settings by the ISP. The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

4.4.5 WAN IP Address Assignment

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

Table 15 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

4.4.6 IP Address and Subnet Mask

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

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

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

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your NBG-417N, 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-417N 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-417N unless you are instructed to do otherwise.

4.4.7 DNS Server Address Assignment

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

The NBG-417N can get the DNS server addresses in the following ways.

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **Wizard** and/or **WAN > Internet Connection** screen.
- 2 If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

4.4.8 WAN IP and DNS Server Address Assignment

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

Figure 20 Wizard Step 3: WAN IP and DNS Server Addresses

The following table describes the labels in this screen

Table 16 Wizard Step 3: WAN IP and DNS Server Addresses

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Enter your WAN IP address in this field. The WAN IP address should be in the same subnet as your DSL/Cable modem or router.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
System DNS Server Address Assignment (if applicable)	
DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The NBG-417N uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.	
First DNS Server	Enter the DNS server's IP address in the fields provided.
Second DNS Server	If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.
Exit	Click Exit to close the wizard screen without saving.

4.4.9 WAN MAC Address

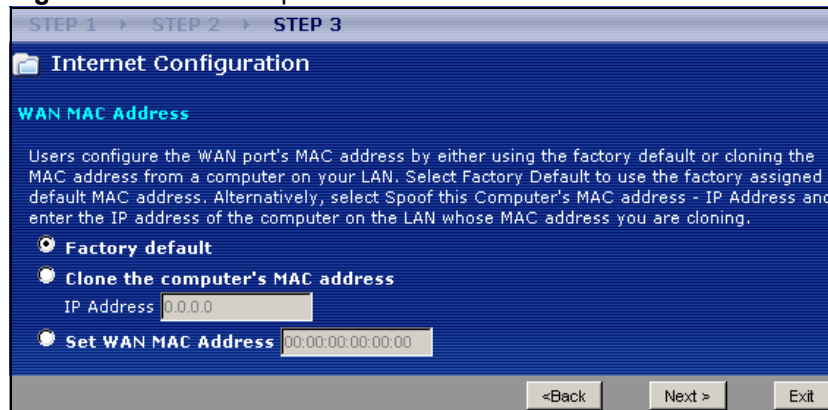
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Table 17 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(NBG-417N LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the NBG-417N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address. Once it is successfully configured, the address will be copied to configuration file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.

Figure 21 Wizard Step 3: WAN MAC Address



The following table describes the fields in this screen.

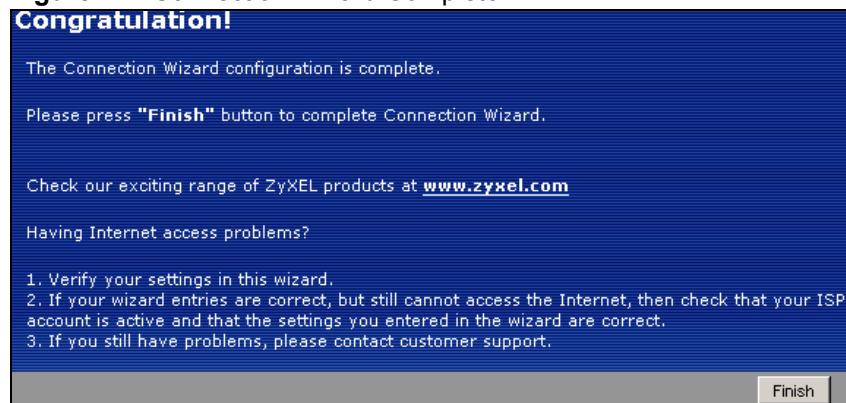
Table 18 Wizard Step 3: WAN MAC Address

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

4.5 Connection Wizard Complete

Click **Finish** to complete the wizard setup.

Figure 22 Connection Wizard Complete



Well done! You have successfully set up your NBG-417N to operate on your network and access the Internet.

5

AP Mode

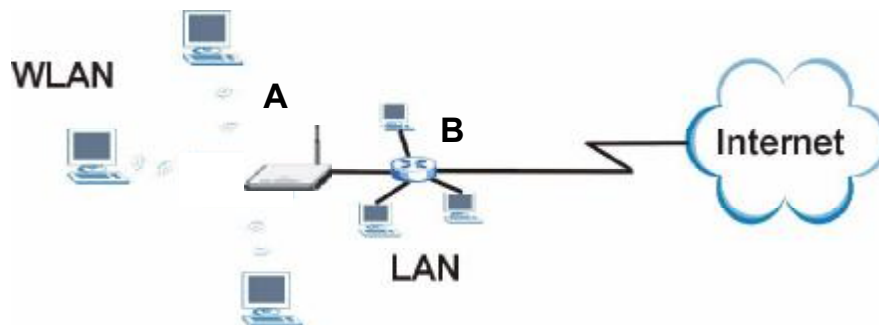
This chapter discusses how to configure settings while your NBG-417N is set to **AP Mode**. Many screens that are available in **Router Mode** are not available in **AP Mode**.

Note: See [Chapter 6 on page 61](#) for an example of setting up a wireless network in AP mode.

5.1 AP Mode Overview

Use your NBG-417N as an AP if you already have a router or gateway on your network. In this mode your device bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 23 Wireless Internet Access in AP Mode

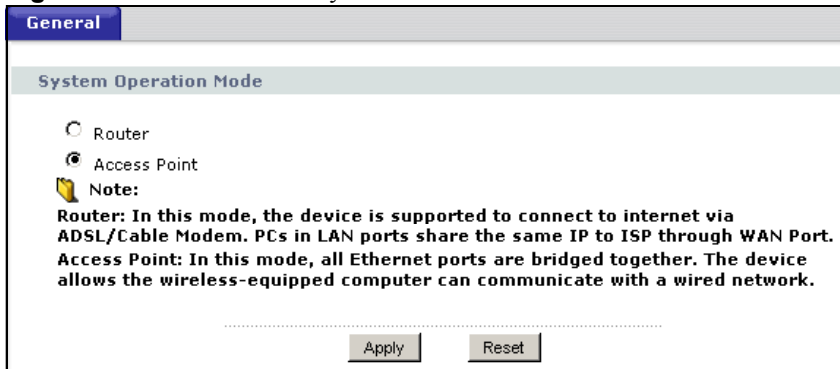


5.2 Setting your NBG-417N to AP Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.

- To set your NBG-417N to **AP Mode**, go to **Maintenance > Sys OP Mode > General** and select **Access Point**.

Figure 24 Maintenance > Sys OP Mode > General



- A pop-up appears providing information on this mode. Click **OK** in the pop-up message window. (See [Section 22.4 on page 191](#) for more information on the pop-up.) Click **Apply**. Your NBG-417N is now in **AP Mode**.

Note: You have to log in to the Web Configurator again when you change modes.

5.3 The Status Screen in AP Mode

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

Figure 25 Status: AP Mode



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

Table 19 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the System Name you enter in the Maintenance > System > General screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - None .
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - On, Off or Off by scheduler .
- Name (SSID)	This shows a descriptive name used to identify the NBG-417N in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG-417N is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG-417N is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the NBG-417N supports. Wireless clients must support the same standard in order to be able to connect to the NBG-417N
- WPS	This shows the WPS (WiFi Protected Setup) Status. Click the status to display Network > Wireless LAN > WPS screen.
System Status	
System Uptime	This is the total time the NBG-417N has been on.
Current Date/Time	This field displays your NBG-417N's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG-417N's processing ability is currently used. When this percentage is close to 100%, the NBG-417N 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-417N is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall.
Interface Status	
Interface	This displays the NBG-417N port types. The port types are: LAN and WLAN .

Table 19 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
Status	For the LAN port, this field displays Down (line is down) or Up (line is up or connected). For the WLAN, it displays Up when the WLAN is enabled or Down when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or N/A when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled.
Summary	
Packet Statistics	Use this screen to view port status and packet specific statistics.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the NBG-417N.

5.3.1 Navigation Panel

Use the menu in the navigation panel to configure NBG-417N features in **AP Mode**.

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

Figure 26 Menu: AP Mode

The following table describes the sub-menus.

Table 20 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG-417N's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		

Table 20 Screens Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG-417N to block access to devices or block the devices from accessing the NBG-417N.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	IP	Use this screen to configure LAN IP address and subnet mask or to get the LAN IP address from a DHCP server.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG-417N's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your NBG-417N.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG-417N.
	Restart	This screen allows you to reboot the NBG-417N without turning the power off.
Sys OP Mode	General	This screen allows you to select whether your device acts as a Router or a Access Point.
Language		This screen allows you to select the language you prefer.

5.4 Configuring Your Settings

5.4.1 LAN Settings

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

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

Note: If you change the IP address of the NBG-417N in the screen below, you will need to log into the NBG-417N again using the new IP address.

Figure 27 Network > LAN > IP

The screenshot shows a web browser window with a blue header bar containing the text 'IP'. Below the header, the page title is 'LAN TCP/IP'. The main content area contains two input fields: 'IP Address' with the value '192.168.1.2' and 'IP Subnet Mask' with the value '255.255.255.0'. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The table below describes the labels in the screen.

Table 21 Network > LAN > IP

LABEL	DESCRIPTION
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-417N 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-417N.
Apply	Click Apply to save your changes to the NBG-417N.
Reset	Click Reset to reload the previous configuration for this screen.

5.4.2 WLAN and Maintenance Settings

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

- See [Chapter 5 on page 69](#) for information on the configuring your wireless network.
- See [Maintenance and Troubleshooting \(173\)](#) for information on the configuring your Maintenance settings.

5.5 Logging in to the Web Configurator in AP Mode

- 1 Connect your computer to the LAN port of the NBG-417N.

- 2 The default IP address of the NBG-417N 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.
- 4 Type "cmd" in the dialog box.
- 5 Type "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix D on page 227](#) for information on changing your computer's IP address.
- 6 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

See [Chapter 6 on page 61](#) for a tutorial on setting up a network with an AP.

Tutorials

This chapter provides tutorials on wireless configurations your NBG-417N.

6.1 How to Connect to the Internet from an AP

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

Figure 28 Wireless AP Connection to the Internet



6.2 Configure Wireless Security Using WPS on both your NBG-417N and Wireless Client

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG-417N 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 6.2.1 on page 62](#). 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-417N's interface. See [Section 6.2.2 on page 63](#). This is the more secure method, since one device can authenticate the other.

6.2.1 Push Button Configuration (PBC)

- 1 Make sure that your NBG-417N 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-417N's Web Configurator and press the **Push Button** button in the **Network > Wireless Client > WPS Station** screen.

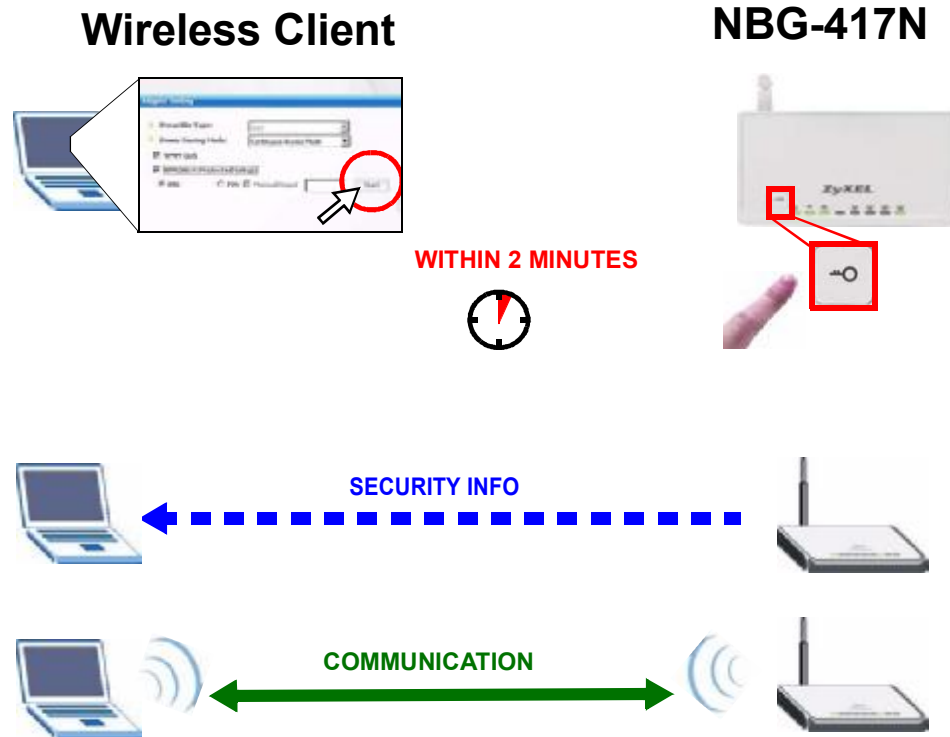
Note: Your NBG-417N has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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-417N 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-417N securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG-417N and wireless client (the NWD210N in this example).

Figure 29 Example WPS Process: PBC Method



6.2.2 PIN Configuration

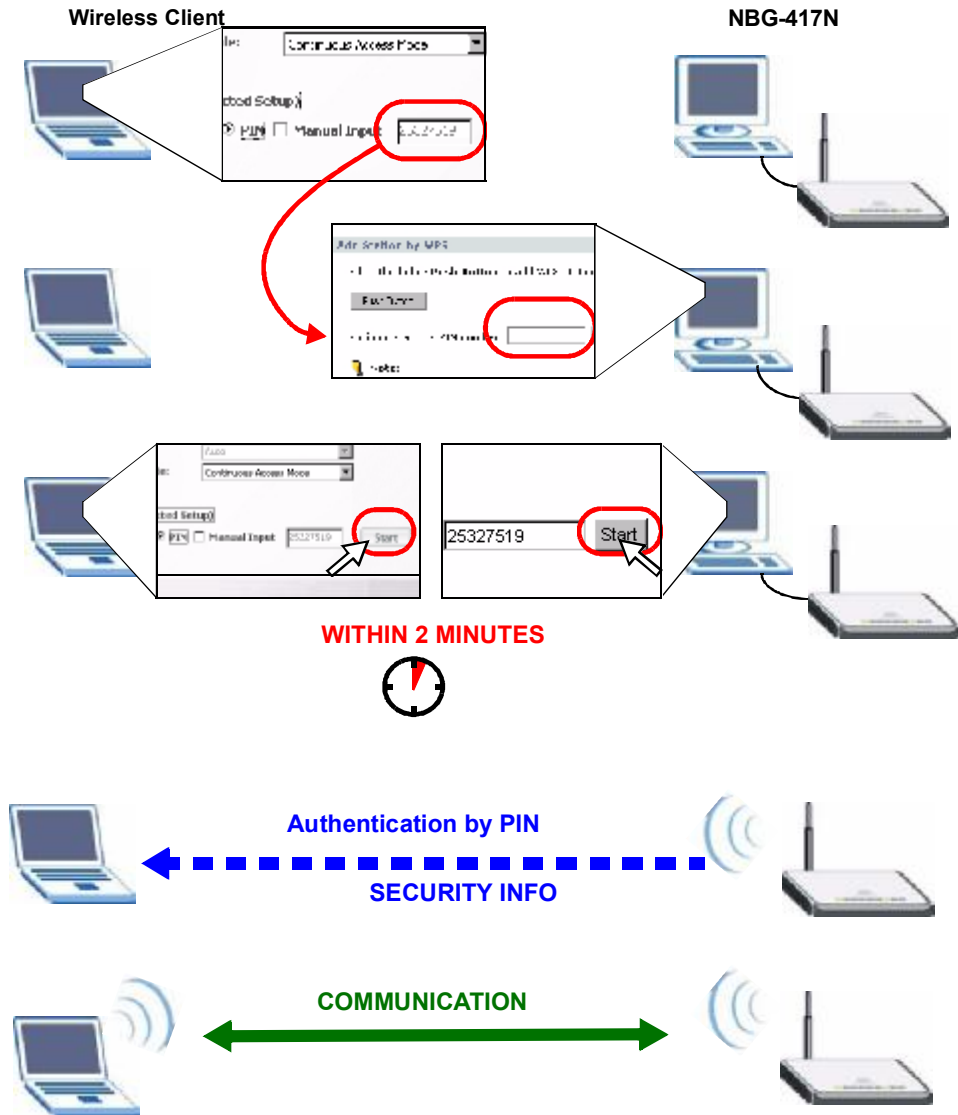
When you use the PIN configuration method, you need to use both NBG-417N's configuration interface and the client's utilities.

- 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-417N.
- 3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG-417N's **WPS Station** screen within two minutes.

The NBG-417N 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-417N securely.

The following figure shows you the example to set up wireless network and security on NBG-417N and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 30 Example WPS Process: PIN Method



6.3 Enable and Configure Wireless Security without WPS on your NBG-417N

This example shows you how to configure wireless security settings with the following parameters on your NBG-417N.

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

Follow the steps below to configure the wireless settings on your NBG-417N.

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 27](#)).

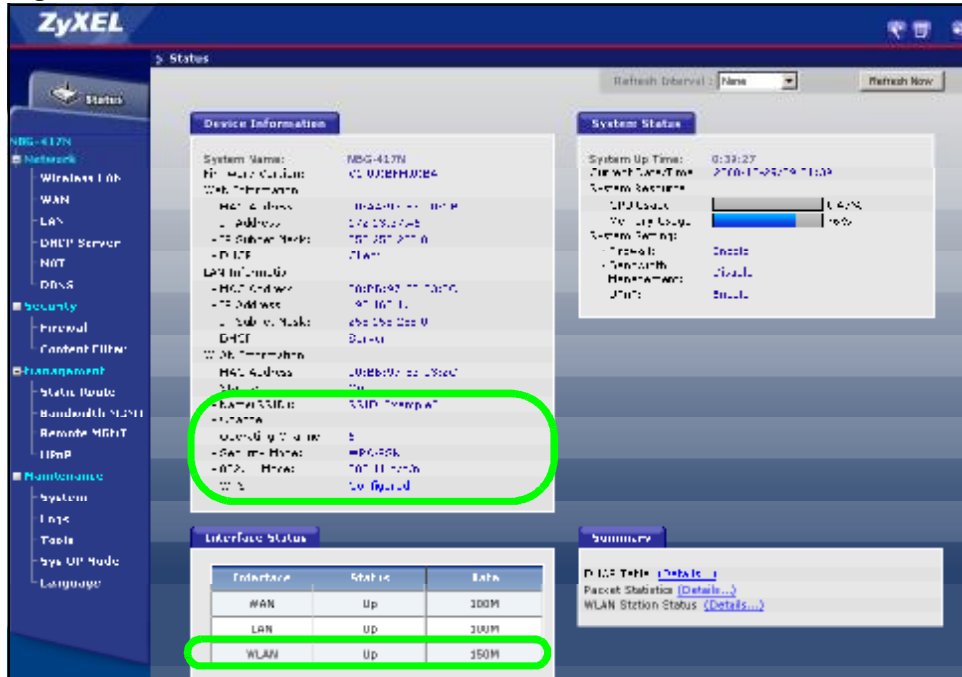
- 1 Open the **Wireless LAN > General** screen in the AP's Web Configurator.
- 2 Make sure the **Enable Wireless LAN** check box is selected.
- 3 Enter **SSID_Example3** as the SSID and select a channel.
- 4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared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

Figure 31 Tutorial: Network > Wireless LAN > General

The screenshot shows the 'Wireless Setup' and 'Security' sections of the Web Configurator. In the 'Wireless Setup' section, the 'Enable Wireless LAN' checkbox is checked. The 'Name(SSID)' field contains 'SSID_Example3'. The 'Channel Selection' is set to 'Channel-06 2437MHz'. In the 'Security' section, the 'Security Mode' is set to 'WPA-PSK' and the 'Pre-Shared Key' is 'ThisismyWPA-PSKpre-sharedkey'. The 'Group Key Update Timer' is set to 180 seconds. A note at the bottom states: 'Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled'. The 'Apply' button is highlighted with a green circle.

- 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 32 Tutorial: Status: AP Mode



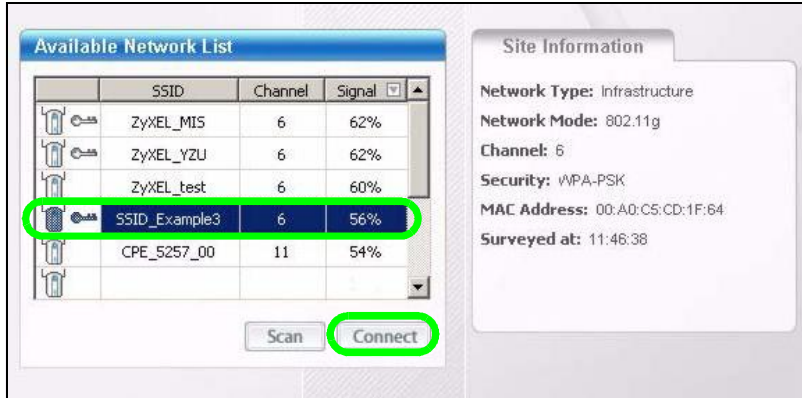
6.4 Configure Your Notebook

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-417N 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.

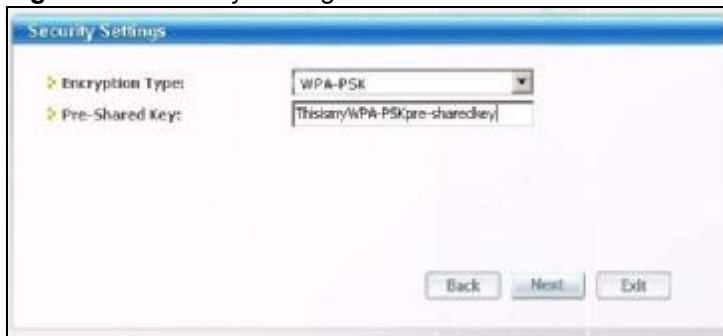
- 4 Select SSID_Example3 and click **Connect**.

Figure 33 Connecting a Wireless Client to a Wireless Network t



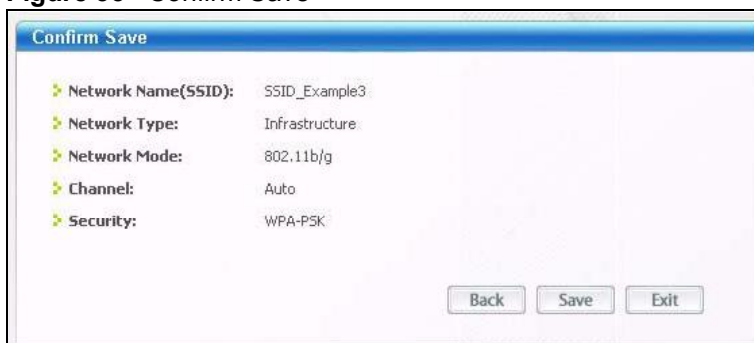
- 5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 34 Security Settings



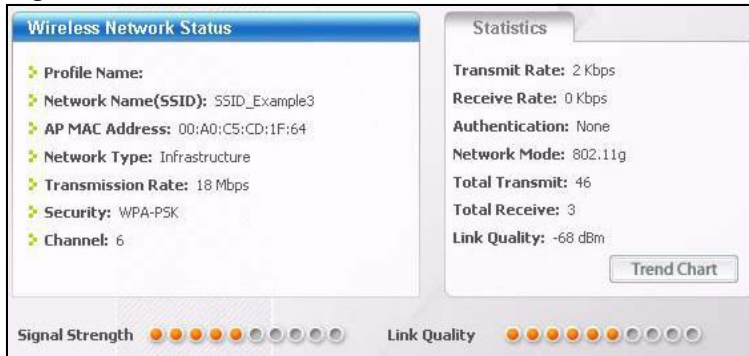
- 6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 35 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 36 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 (71)

WAN (91)

LAN (103)

DHCP Server (107)

Network Address Translation (NAT) (113)

Dynamic DNS (123)

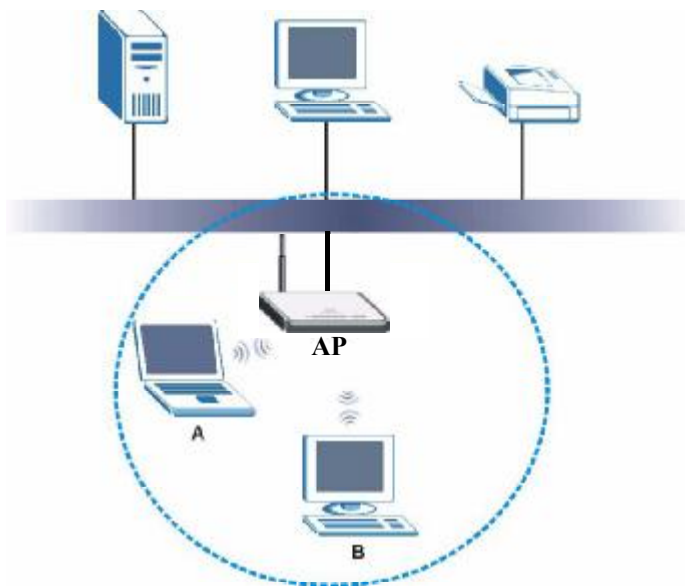
Wireless LAN

7.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG-417N. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 37 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-417N is the AP.

7.2 What You Can Do In the Wireless LAN Screen

- Use the **General** screen ([Section 7.4 on page 75](#)) to enable the Wireless LAN, enter the SSID and select the wireless security mode.
- Use the **MAC Filter** screen ([Section 7.5 on page 80](#)) to allow or deny wireless stations based on their MAC addresses from connecting to the NBG-417N.
- Use the **Advanced** screen ([Section 7.6 on page 82](#)) to allow intra-BSS networking and set the RTS/CTS Threshold.
- Use the **QoS** screen ([Section 7.7 on page 83](#)) to set priority levels to services, such as e-mail, VoIP, chat, and so on.
- Use the **WPS** screen ([Section 7.8 on page 87](#)) to quickly set up a wireless network with strong security, without having to configure security settings manually.
- Use the **WPS Station** screen ([Section 7.9 on page 88](#)) to add a wireless station using WPS.
- Use the **Scheduling** screen ([Section 7.10 on page 88](#)) to set the times your wireless LAN is turned on and off.

7.3 What You Should Know About Wireless LAN

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

7.3.1 Wireless Security Overview

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

7.3.1.1 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.

7.3.1.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

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

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

7.3.1.3 User Authentication

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

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

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

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

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

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.


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

7.3.1.4 Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See [Section 7.3.1.3 on page 73](#) for information about this.)

Table 22 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest  Strongest	No Security	WPA
	Static WEP	
	WPA-PSK	
	WPA2-PSK	WPA2

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

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

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

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

When you select **WPA2** or **WPA2-PSK** in your NBG-417N, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the NBG-417N.

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

7.3.1.5 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 6.2 on page 61](#).

7.4 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-417N from a computer connected to the wireless LAN and you change the NBG-417N'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-417N's new settings.

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

Figure 38 Network > Wireless LAN > General

The screenshot shows the configuration interface for the Wireless LAN. The 'General' tab is selected. The 'Wireless Setup' section includes:

- Enable Wireless LAN
- Name(SSID):
- Hide SSID
- Channel Selection: Auto Channel Selection
- Operating Channel:
- Channel Width:

 The 'Security' section shows:

- Security Mode:

 A note with a warning icon states: "Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled". At the bottom, there are 'Apply' and 'Reset' buttons.

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

Table 23 Network > Wireless LAN > General

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if Auto Channel Selection is disabled.
Auto Channel Selection	Select this check box for the NBG-417N to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the Channel Section field.
Operating Channel	This displays the channel the NBG-417N is currently using.
Channel Width	Select whether the NBG-417N uses a wireless channel width of 20 or 40 MHz. A standard 20 MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. Because not all devices support 40 MHz channels, select Auto 20/40MHz to allow the NBG-417N to adjust the channel bandwidth automatically.
Security Mode	Select WPA-PSK or WPA2-PSK to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See 7.4.2 and 7.4.3 sections. Or you can select No Security to allow any client to associate this network without authentication. Note: If you enable the WPS function, only No Security , WPA-PSK and WPA2-PSK are available in this field.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to reload the previous configuration for this screen.

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

7.4.1 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-417N, your network is accessible to any wireless networking device that is within range.

Figure 39 Network > Wireless LAN > General: No Security

The screenshot shows the 'General' tab of the 'Wireless LAN' configuration page. Under 'Wireless Setup', the 'Enable Wireless LAN' checkbox is checked. The 'Name(SSID)' field contains 'SSID_Example3'. The 'Hide SSID' checkbox is unchecked. 'Channel Selection' is set to 'Channel-06 2437MHz' and 'Auto Channel Selection' is unchecked. 'Operating Channel' is 'Channel-6' and 'Channel Width' is 'Auto 20/40 MHz'. Under 'Security', the 'Security Mode' dropdown is set to 'No security'. A note with a yellow icon says 'Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled'. At the bottom are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 24 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose No Security from the drop-down list box.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to reload the previous configuration for this screen.

7.4.2 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-417N 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 40 Network > Wireless LAN > General: Static WEP

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

Table 25 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
WEP Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	This field is activated when you select 64-bit WEP or 128-bit WEP in the WEP Encryption field. Select Auto , Open System or Shared Key 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 Auto or Open System unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select Shared Key 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.

Table 25 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
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-417N and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to reload the previous configuration for this screen.

7.4.3 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 41 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

The screenshot displays the configuration interface for WPA-PSK/WPA2-PSK. The 'General' tab is selected, showing the following settings:

- Wireless Setup:**
 - Enable Wireless LAN
 - Name(SSID): SSID_Example3
 - Hide SSID
 - Channel Selection: Channel-06 2437MHz (dropdown)
 - Operating Channel: Channel-6
 - Channel Width: Auto 20/40 MHz (dropdown)
 - Auto Channel Selection
- Security:**
 - Security Mode: WPA2-PSK (dropdown)
 - WPA Compatible
 - Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey
 - Group Key Update Timer: 600 (In Seconds)
 - Radio buttons: ASCII, Hex

A note at the bottom states: **Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled**. Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

The following table describes the labels in this screen.

Table 26 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG-417N even when the NBG-417N is using WPA2-PSK.
Pre-Shared Key	WPA-PSK/WPA2-PSK uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). Type a pre-shared key less than 64 case-sensitive HEX characters ("0-9", "A-F").
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA/WPA2 key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. The default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to reload the previous configuration for this screen.

7.5 MAC Filter

The MAC filter screen allows you to configure the NBG-417N to give exclusive access to up to 16 devices (Allow) or exclude up to 16 devices from accessing the NBG-417N (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-417N's MAC filter settings, click **Network > Wireless LAN > MAC Filter**. The screen appears as shown.

Figure 42 Network > Wireless LAN > MAC Filter

The following table describes the labels in this menu.

Table 27 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Select Yes from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC Address table. Select Deny to block access to the NBG-417N, MAC addresses not listed will be allowed to access the NBG-417N Select Allow to permit access to the NBG-417N, MAC addresses not listed will be denied access to the NBG-417N.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the NBG-417N in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to reload the previous configuration for this screen.

7.6 Wireless LAN Advanced Screen

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

Figure 43 Network > Wireless LAN > Advanced

The following table describes the labels in this screen.

Table 28 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 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 256 and 2346 . This field is not available when Super Mode is selected.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the NBG-417N does, it cannot communicate with the NBG-417N.

Table 28 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
CTS Protection	<p>When set to None, the NBG-417N protects wireless communication against interference.</p> <p>When set to Always, the NBG-417N improves performance within mixed wireless modes.</p> <p>Select Auto to let the NBG-417N determine whether to turn this feature on or off in the current environment.</p>
Tx Power	<p>This field controls the transmission power of the NBG-417N. When using the NBG-417N with a notebook computer, select a lower transmission power level when you are close to the AP in order to conserve battery power.</p>
Enable Intra-BSS Traffic	<p>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).</p> <p>Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client A and B can still access the wired network but cannot communicate with each other.</p>
Apply	<p>Click Apply to save your changes back to the NBG-417N.</p>
Reset	<p>Click Reset to reload the previous configuration for this screen.</p>

7.7 Quality of Service (QoS) Screen

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

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

Figure 44 Network > Wireless LAN > QoS

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

The following table describes the labels in this screen.

Table 29 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
WMM QoS Policy	Select Default to have the NBG-417N automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Select Application Priority from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS. The table appears only if you select Application Priority in WMM QoS Policy .
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either FTP , WWW , E-mail or a User Defined service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.

Table 29 Network > Wireless LAN > QoS (continued)

LABEL	DESCRIPTION
Priority	This field displays the priority of the application. Highest - Typically used for voice or video that should be high-quality. High - Typically used for voice or video that can be medium-quality. Mid - Typically used for applications that do not fit into another priority. For example, Internet surfing. Low - Typically used for non-critical "background" applications, such as large file transfers and print jobs that should not affect other applications.
Modify	Click the Edit icon to open the Application Priority Configuration screen. Modify an existing application entry or create a application entry in the Application Priority Configuration screen. Click the Remove icon to delete an application entry.
Apply	Click Apply to save your changes to the NBG-417N.

7.7.1 Application Priority Configuration

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

Figure 45 Network > Wireless LAN > QoS: Application Priority Configuration

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

Network > Wireless LAN > QoS: Application Priority Configuration

LABEL	DESCRIPTION
Name	Type a description of the application priority.

Network > Wireless LAN > QoS: Application Priority Configuration (continued)

LABEL	DESCRIPTION
Service	<p>The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box.</p> <ul style="list-style-type: none"> • E-Mail <p>Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail:</p> <p>POP3 - port 110</p> <p>IMAP - port 143</p> <p>SMTP - port 25</p> <p>HTTP - port 80</p> <ul style="list-style-type: none"> • FTP <p>File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21.</p> <ul style="list-style-type: none"> • WWW <p>The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.</p> <ul style="list-style-type: none"> • User-Defined <p>User-defined services are user specific services configured using known ports and applications.</p>
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click Apply to save your changes back to the NBG-417N.
Cancel	Click Cancel to return to the previous screen.

7.8 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 46 WPS

The following table describes the labels in this screen.

Table 30 WPS

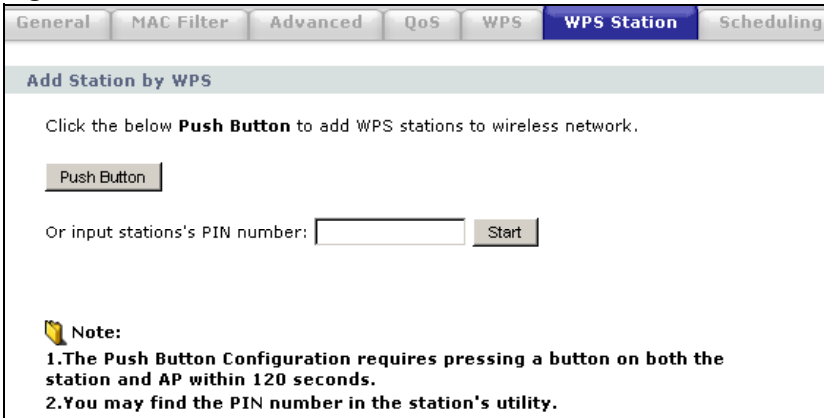
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click Generate to generate a new PIN number.
WPS Status	
Status	This displays Configured when the NBG-417N has connected to a wireless network using WPS or when Enable WPS 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 Unconfigured if WPS is disabled and there are no wireless or wireless security changes on the NBG-417N or you click Release_Configuration to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays Configured . Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG-417N.
Apply	Click Apply to save your changes back to the NBG-417N.
Refresh	Click Refresh to get this screen information afresh.

7.9 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 47 WPS Station



The following table describes the labels in this screen.

Table 31 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 Section 6.2.1 on page 62 . 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 Section 6.2.2 on page 63 . Type the same PIN number generated in the wireless station's utility. Then click Start to associate to each other and perform the wireless security information synchronization.

7.10 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 48 Scheduling

Action	Day	Except for the following times
<input type="radio"/> On <input checked="" type="radio"/> Off	<input 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)

The following table describes the labels in this screen.

Table 32 Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Action	Select On or Off to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the Day and Except for the following times fields.
Day	Select Everyday or the specific days to turn the Wireless LAN on or off. If you select Everyday you can not select any specific days. This field works in conjunction with the Except for the following times field.
Except for the following times (24-Hour Format)	Select a begin time using the first set of hour and minute (min) drop down boxes and select an end time using the second set of hour and minute (min) drop down boxes. If you have chosen On earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. If you have chosen Off earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. Note: Entering the same begin time and end time will mean the whole day.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to reload the previous configuration for this screen.

8

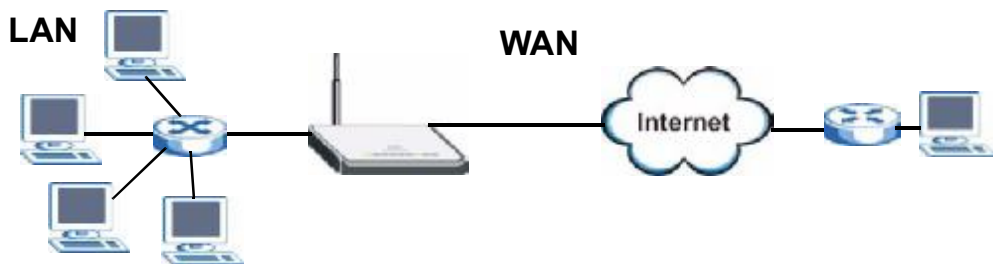
WAN

8.1 Overview

This chapter discusses the NBG-417N's **WAN** screens. Use these screens to configure your NBG-417N 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 49 LAN and WAN



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

8.2 What You Can Do In the WAN Screens

- Use the **Internet Connection** ([Section 8.4 on page 95](#)) screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses.
- Use the **Advanced** ([Section 8.5 on page 101](#)) screen to enable multicasting, configure Windows networking and bridge.

8.3 What You Need To Know About WAN

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-417N.

8.3.1 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-417N, which makes it accessible from an outside network. It is used by the NBG-417N to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG-417N 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 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-417N 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-417N's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

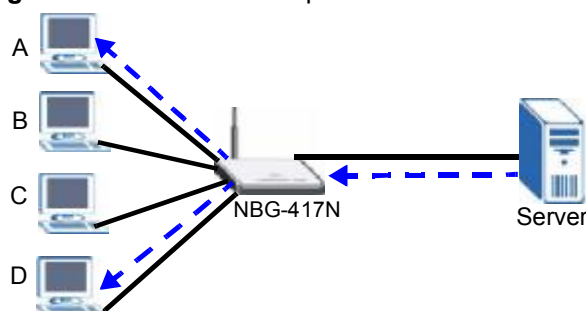
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

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.

8.3.2 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 50 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-417N supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the NBG-417N queries all directly connected networks to gather group membership. After that, the NBG-417N periodically updates this information. IP multicasting can be enabled/disabled on the NBG-417N LAN and/or WAN interfaces in the Web Configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

8.3.3 NetBIOS over TCP/IP

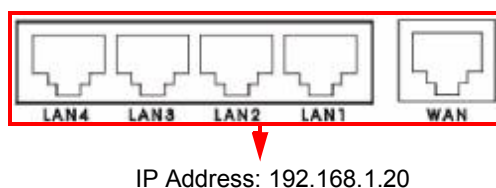
NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.

8.3.4 Auto-Bridge

In the rear panel of your NBG-417N, you can see four LAN ports (1 to 4) and one WAN port. The WAN port is for your Internet access connection, and the LAN ports are for your network devices. The WAN port has a different IP address from the LAN ports.

When you enable auto-bridging in your NBG-417N, all five ports (4 LAN ports and the WAN port) share the same IP address as shown in the figure below.

Figure 51 Autobridging Example



This might happen if you put the NBG-417N behind a NAT router that assigns it this IP address. When the NBG-417N is in auto-bridge mode, the NBG-417N acts as an AP and all the interfaces (LAN, WAN and WLAN) are bridged. In this mode, your NAT, DHCP server, firewall and bandwidth management (rules) on the NBG-417N are not available. You do not have to reconfigure them if you return to router mode.

Auto-bridging only works under the following conditions:

- The WAN IP must be 192.168.x.y (where x and y must be from zero to nine). If the LAN IP address and the WAN IP address are in the same subnet but x or y is greater than nine, the device operates in router mode (with firewall and bandwidth management available).
- The device must be in **Router Mode** (see [Chapter 22 on page 189](#) for more information) for auto-bridging to become active.

8.4 Internet Connection

Use this screen to change your NBG-417N's Internet access settings. Click **Network** > **WAN**. The screen differs according to the encapsulation you choose.

8.4.1 Ethernet Encapsulation

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

Figure 52 Network > WAN > Internet Connection: Ethernet Encapsulation

The following table describes the labels in this screen.

Table 33 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
Connection Type	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
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.

Table 33 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
IP Subnet Mask	Enter the IP Subnet Mask in this field.
Gateway IP Address	Enter a Gateway IP Address (if your ISP gave you one) in this field.
DNS Servers	
First DNS Server Second DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the NBG-417N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG-417N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

8.4.2 PPPoE Encapsulation

The NBG-417N 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-417N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG-417N 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 53 Network > WAN > Internet Connection: PPPoE Encapsulation

The following table describes the labels in this screen.

Table 34 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select PPP over Ethernet if you connect to your Internet via dial-up.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.

Table 34 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
DNS Servers	
First DNS Server	Select From ISP if your ISP dynamically assigns DNS server information (and the NBG-417N'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 User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the NBG-417N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

8.4.3 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 54 Network > WAN > Internet Connection: PPTP Encapsulation

The screenshot shows the 'Internet Connection' configuration window with the 'Advanced' tab selected. The 'Connection Type' is set to 'PPTP'. Under 'ISP Parameters for Internet Access', there are fields for 'User Name', 'Password', and 'Encryption Confirmation', along with a checked 'Require IP Connection' and a 'Idle Timeout' of 300 seconds. The 'PPTP Configuration' section includes 'Server IP Address/Domain' and 'Connection ID/Name' fields, and radio buttons for 'Get automatically from ISP' (unchecked) and 'Use local IP Address' (checked). Below this are fields for 'WAN IP Address' and 'IP Subnet Mask'. The 'WAN IP Address Assignment' section has a radio button for 'Get automatically from ISP' (checked). The 'DNS Servers' section has 'First DNS Server' and 'Secondary DNS Server' fields, both set to 'From ISP' with IP addresses 172.28.5.2 and 172.28.5.1. The 'WAN MAC Address' section has radio buttons for 'Factory default' (checked), 'Clone the computer's MAC address - IP Address' (with IP address 1.1.1.1), and 'Set WAN MAC Address' (with address 00:00:00:00:00:00). 'Apply' and 'Reset' buttons are at the bottom.

The following table describes the labels in this screen.

Table 35 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The NBG-417N supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.

Table 35 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
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 Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the NBG-417N automatically disconnects from the PPTP server.
PPTP Configuration	
Server IP Address/ Domain	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for 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.
My WAN IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
My IP Subnet Mask	Your NBG-417N 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-417N.
WAN IP Address Assignment	
Get automatically from ISP	Select this to get your WAN IP address from your ISP.
DNS Servers	
First DNS Server Second DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the NBG-417N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG-417N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.

Table 35 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
Clone the computer's MAC address - IP Address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

8.5 Advanced WAN Screen

Use this screen to enable **Multicast**, allow **Windows Networking** and enable **Auto-bridge**.

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

To change your NBG-417N's advanced WAN settings, click **Network > WAN > Advanced**. The screen appears as shown.

Figure 55 Network > WAN > Advanced

The screenshot shows the 'Advanced' configuration screen for WAN settings. It is divided into three main sections, each with a checkbox:

- Multicast Setup:** Contains a checkbox labeled 'Multicast'.
- Windows Networking (NetBIOS over TCP/IP):** Contains two checkboxes: 'Allow between LAN and WAN' and 'Allow Trigger Dial'.
- Auto-bridge:** Contains a checkbox labeled 'Enable Auto-bridge mode'.

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

The following table describes the labels in this screen.

Table 36 WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	<p>Check this to enable multicasting. This applies to traffic routed from the WAN to the LAN.</p> <p>Leaving this blank may cause incoming traffic to be dropped or sent to all connected network devices.</p>
Windows Networking (NetBIOS over TCP/IP)	
Allow between LAN and WAN	<p>Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.</p>
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Auto-bridge	
Enable Auto-bridge mode	Select this option to have the NBG-417N switch to bridge mode automatically when the NBG-417N 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 Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

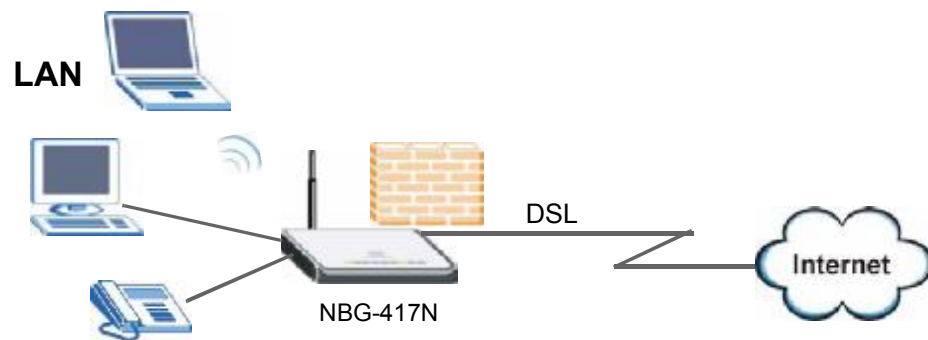
9

LAN

9.1 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.



The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

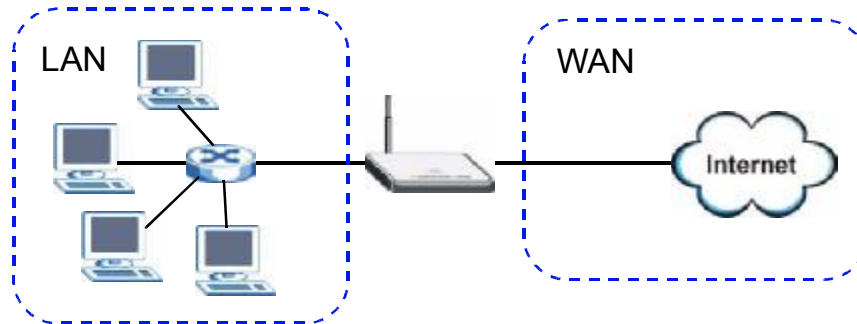
9.2 What You Can Do in the LAN Screen

Use the [IP \(Section 9.4 on page 105\)](#) screen to change your basic LAN settings.

9.3 What You Need To Know About LAN

The actual physical connection determines whether the NBG-417N 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 56 LAN and WAN IP Addresses



The LAN parameters of the NBG-417N 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.

9.3.1 IP Pool Setup

The NBG-417N 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-417N 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.

Refer to [Section 4.4.6 on page 48](#) for information on IP Address and Subnet Mask.

9.3.2 LAN TCP/IP

The NBG-417N has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

Refer to the [Section 4.4.7 on page 49](#) section for information on System DNS Servers.

9.4 LAN IP Screen

Use this screen to change your basic LAN settings. Click **Network** > **LAN**.

Figure 57 Network > LAN > IP

The following table describes the labels in this screen.

Table 37 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your NBG-417N in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG-417N 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-417N.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

DHCP Server

10.1 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-417N's LAN as a DHCP server or disable it. When configured as a server, the NBG-417N 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.

10.2 What You Can Do in the DHCP Server Screens

- Use the **General** ([Section 10.4 on page 108](#)) screen to enable the DHCP server.
- Use the **Advanced** ([Section 10.5 on page 108](#)) screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
- Use the **Client List** ([Section 10.6 on page 110](#)) screen to view the current DHCP client information.

10.3 What You Need To Know About the DHCP Server Screens

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. Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

Refer to [Section 4.4.6 on page 48](#) for information on IP Address and Subnet Mask.

Refer to the [Section 4.4.7 on page 49](#) section for information on System DNS Servers.

10.4 General Screen

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

Figure 58 Network > DHCP Server > General

The screenshot shows a web interface for configuring the DHCP server. At the top, there are three tabs: 'General' (selected), 'Advanced', and 'Client List'. Below the tabs is a 'DHCP Setup' section. It contains a checked checkbox labeled 'Enable DHCP Server'. Below this, there are two input fields: 'IP Pool Starting Address' with the value '192.168.1.33' and 'Pool Size' with the value '32'. At the bottom right of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 38 Network > DHCP Server > General

LABEL	DESCRIPTION
Enable DHCP Server	Enable or Disable DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the Enable DHCP Server check box selected unless your ISP instructs you to do otherwise. Clear it to disable the NBG-417N acting as a DHCP server. When configured as a server, the NBG-417N provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
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 Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

10.5 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-417N sends to the DHCP clients.

To change your NBG-417N's static DHCP settings, click **Network > DHCP Server > Advanced**. The following screen displays.

Figure 59 Network > DHCP Server > Advanced

The following table describes the labels in this screen.

Table 39 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
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-417N passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG-417N only passes this information to the LAN DHCP clients when you select the Enable DHCP Server check box. When you clear the Enable DHCP Server 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.

Table 39 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
First DNS Server Second DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the NBG-417N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select DNS Relay to have the NBG-417N act as a DNS proxy. The NBG-417N's LAN IP address displays in the field to the right (read-only). The NBG-417N tells the DHCP clients on the LAN that the NBG-417N itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG-417N, the NBG-417N forwards the query to the NBG-417N's system DNS server (configured in the WAN > Internet Connection screen) and relays the response back to the computer. You can only select DNS Relay for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

10.6 Client List Screen

The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of network clients using the NBG-417N's DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network > DHCP Server > Client List**.

Note: You can also view a read-only client list by clicking the **DHCP Table (Details...)** hyperlink in the **Status** screen.

The following screen displays.

Figure 60 Network > DHCP Server > Client List

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	T09C13762 71	08:00:C4:84:F1:43	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 40 Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select this check box in the DHCP Setup section to have the NBG-417N always assign the IP address(es) to the MAC address(es) (and host name(s)). After you click Apply , the MAC address and IP address also display in the Advanced screen (where you can edit them).
Apply	Click Apply to save your settings.
Refresh	Click Refresh to reload the DHCP table.

Network Address Translation (NAT)

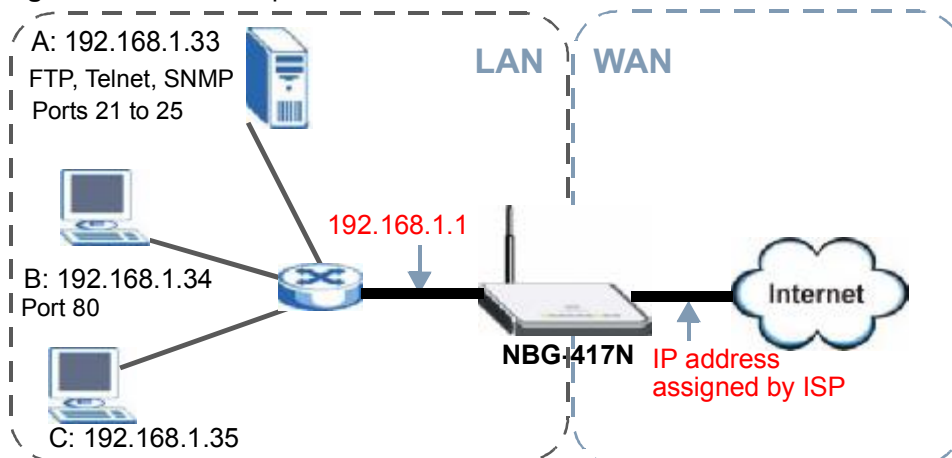
11.1 Overview

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.

The figure below is a simple illustration of a NAT network. You want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example).

You assign the LAN IP addresses to the devices (**A** to **D**) connected to your NBG-417N. The ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet. All traffic coming from **A** to **D** going out to the Internet use the IP address of the NBG-417N, which is 192.168.1.1.

Figure 61 NAT Example



This chapter discusses how to configure NAT on the NBG-417N.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG-417N.

11.2 What You Can Do in the NAT Screens

- Use the **General** ([Section 11.4 on page 116](#)) screen to enable NAT and set a default server.
- Use the **Application** ([Section 11.5 on page 117](#)) screen to change your NBG-417N's port forwarding settings.
- Use the **Advanced** ([Section 11.9 on page 121](#)) screen to change your NBG-417N's trigger port settings.

11.3 What You Need To Know About NAT

Read on for basic information on NAT and for details that can help you understand and configure the NAT screens of your NBG-417N.

Note the following definitions that are used in this section.

Inside/outside

This denotes where a host is located relative to the NBG-417N, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local

This denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note: Inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet.

An inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the

IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 41 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

11.3.1 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

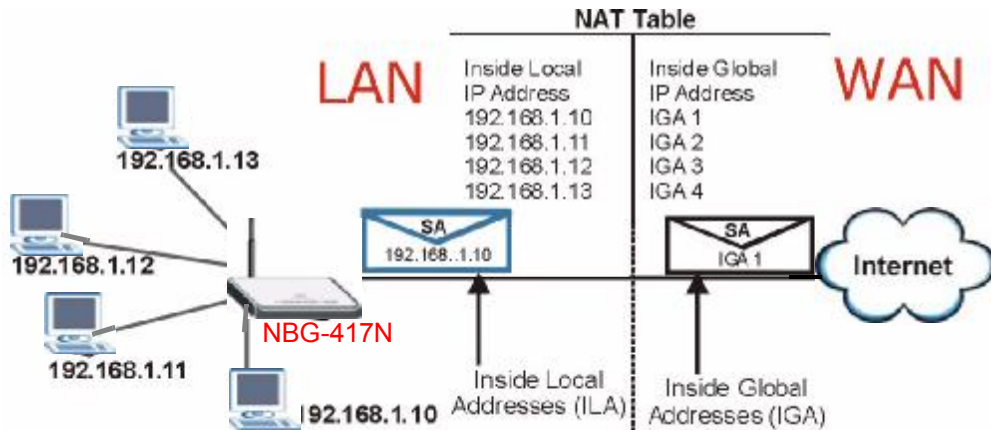
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your NBG-417N filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

11.3.2 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. 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-417N 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 62 How NAT Works



11.4 General NAT Screen

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

Figure 63 Network > NAT > General

General	Application	Advanced
NAT Setup		
<input checked="" type="checkbox"/> Enable Network Address Translation		
Default Server Setup		
Server IP Address	<input type="text" value="0.0.0.0"/>	
		<input type="button" value="Apply"/> <input type="button" value="Reset"/>

The following table describes the labels in this screen.

Table 42 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.

Table 42 Network > NAT > General

LABEL	DESCRIPTION
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 Application screen. If you do not assign a Default Server IP address , the NBG-417N discards all packets received for ports that are not specified in the Application screen or remote management.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

11.5 NAT Application Screen

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG-417N'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-417N discards all packets received for ports that are not specified in this screen or remote management.

Refer to [Appendix F on page 257](#) for port numbers commonly used for particular services.

Figure 64 Network > NAT > Application

The screenshot shows the 'Application' configuration screen. At the top, there are tabs for 'General', 'Application', and 'Advanced'. The 'Application' tab is active. Below the tabs, there is a section titled 'Add Application Rule' with a 'Service' dropdown menu set to 'user-defined'. Below this are input fields for 'Local Port Range', 'Public Port Range', and 'Server IP Address', along with 'Apply' and 'Cancel' buttons. Below the configuration fields is a table titled 'Application Rules Summary' with the following columns: #, Active, Name, Local (Start Port, End Port), Public (Start Port, End Port), Server IP Address, and Modify. The table contains 10 rows, numbered 1 through 10, each with an 'Active' status icon and a 'Modify' icon.

#	Active	Name	Local		Public		Server IP Address	Modify
			Start Port	End Port	Start Port	End Port		
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

The following table describes the labels in this screen.

Table 43 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 Service Name . Otherwise, select a predefined service in the second field next to Service Name . The predefined service name and port number(s) will display in the Service Name and Port fields.
Local Port Range Public Port Range	Type a port number(s) to be forwarded. 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 inside IP address of the server that receives packets from the port(s) specified in the Port field.
Apply	Click Apply to save your changes to the Application Rules Summary table.
Reset	Click Reset to not save and return your new changes in the Service Name and Port fields to the previous one.
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.
Local Start/End Port Public Start/End Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the Edit icon to display and modify an existing rule setting in the fields under Add Application Rule . Click the Remove icon to delete a rule.

11.6 NAT Advanced Screen

To change your NBG-417N'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 65 Network > NAT > Advanced

The screenshot shows the 'Advanced' tab of the NAT configuration interface. It features a table titled 'Port Triggering Rules' with 10 rows. Each row has columns for a rule number, a name, and two sets of port ranges: 'Incoming' (Start Port and End Port) and 'Trigger' (Start Port and End Port). Below the table are 'Apply' and 'Reset' buttons.

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

The following table describes the labels in this screen.

Table 44 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-417N 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-417N 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.

Table 44 Network > NAT > Advanced

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

11.7 Technical Reference

The following section contains additional technical information about the NBG-417N features described in this chapter.

11.8 Using NATPort Forwarding: Services and Port Numbers

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

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.

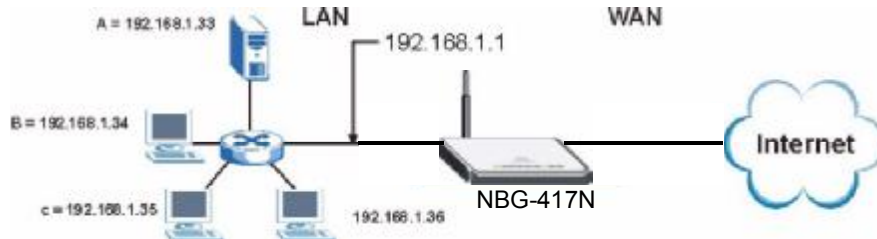
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your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

11.8.1 Configuring Servers Behind Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP

address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 66 Multiple Servers Behind NAT Example



11.9 Trigger Port Forwarding

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-417N 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-417N's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG-417N 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.

11.9.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 67 Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the NBG-417N to record Jane's computer IP address. The NBG-417N 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-417N 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-417N times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

11.9.2 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is going coming from inside the NBG-417N and going to the outside.
- 2 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.

Dynamic DNS

12.1 Overview

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

12.2 What You Can Do in the DDNS Screen

Use the **Dynamic DNS** screen ([Section 12.4 on page 124](#)) to enable DDNS and configure the DDNS settings on the NBG-417N.

12.3 What You Need To Know About DDNS

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.

12.3.1 DynDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, [www.yourhost.dyndns.org](#) and still reach your hostname.

Note: If you have a private WAN IP address, then you cannot use Dynamic DNS. You must have a public WAN IP address.

12.4 Dynamic DNS Screen

To change your NBG-417N's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 68 Dynamic DNS

The following table describes the labels in this screen.

Table 45 Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from 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.
Token	Enter your client authorization key provided by the server to update DynDNS records. This field is configurable only when you select WWW.REGFISH.COM in the Service Provider field.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.

Table 45 Dynamic DNS

LABEL	DESCRIPTION
Enable off line option	This option is available when CustomDNS is selected in the DDNS Type field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

PART III

Security

Firewall (129)

Content Filtering (135)

Firewall

13.1 Overview

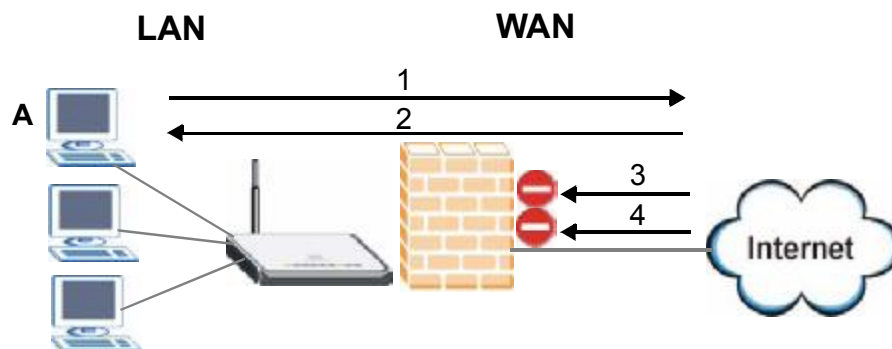
Use these screens to enable and configure the firewall that protects your NBG-417N and your LAN from unwanted or malicious traffic.

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 69 Default Firewall Action



13.2 What You Can Do in the Firewall Screens

- Use the **General** ([Section 13.4 on page 132](#)) screen to enable or disable the NBG-417N's firewall.
- Use the Services () screen to

13.3 What You Need To Know About Firewall

The NBG-417N's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

13.3.1 What is a Firewall?

Originally, the term "firewall" referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

13.3.2 Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

13.3.3 About the NBG-417N Firewall

The NBG-417N firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The NBG-417N's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG-417N 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-417N 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-417N 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.

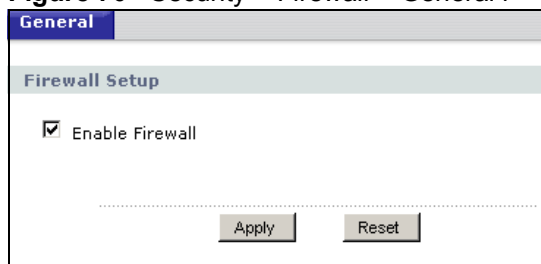
13.3.4 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via Web Configurator.
- 2 Think about access control before you connect to the network in any way, including attaching a modem to the port.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

13.4 General Firewall Screen

Use this screen to enable or disable the NBG-417N's firewall, and set up firewall logs. Click **Security > Firewall** to open the **General** screen.

Figure 70 Security > Firewall > General I



The following table describes the labels in this screen.

Table 46 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The NBG-417N performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen again.

13.5 Services Screen

If an outside user attempts to probe an unsupported port on your NBG-417N, an ICMP response packet is automatically returned. This allows the outside user to know the NBG-417N exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG-417N 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 71 Security > Firewall > Services I

The screenshot shows a configuration window with two tabs: 'General' and 'Services'. The 'Services' tab is active. Under the 'ICMP' section, there is a 'Respond to Ping on' dropdown menu currently set to 'LAN'. Below it is a checked checkbox labeled 'Do not respond to requests for unauthorized services'. At the bottom of the window are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 47 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-417N will not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN & WAN to reply to all incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the NBG-417N by probing for unused ports. If you select this option, the NBG-417N will not respond to port request(s) for unused ports, thus leaving the unused ports and the NBG-417N unseen. By default this option is not selected and the NBG-417N will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the NBG-417N's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the NBG-417N reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcrst rst [on off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen again.

Content Filtering

14.1 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.

14.2 What You Can Do in the Content Filtering Screen

Use the **Filter** ([Section 14.4 on page 137](#)) screen to restrict web features, add keywords for blocking and designate a trusted computer.

14.3 What You Need To Know About Content Filtering

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.

14.3.1 Content Filtering Profiles

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

Restrict Web Features

The NBG-417N can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.

Keyword Blocking URL Checking

The NBG-417N 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, the domain name is www.zyxel.com.tw.

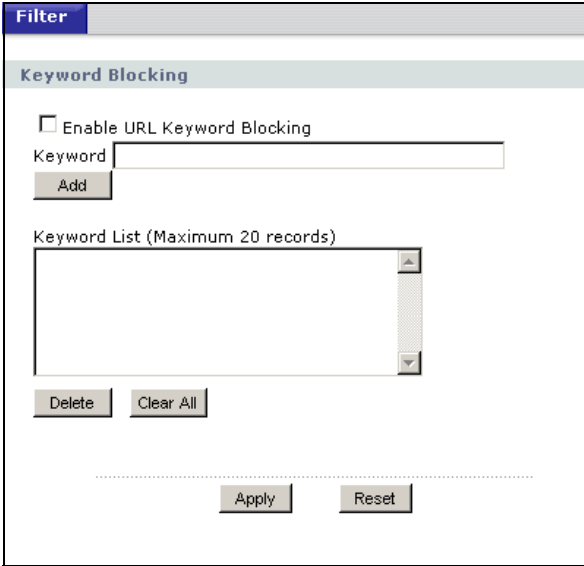
The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is [news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php).

Since the NBG-417N 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, the NBG-417N would find "tw" in the domain name (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".

14.4 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 **Filter** screen.

Figure 72 Security > Content Filter > Filter



The following table describes the labels in this screen.

Table 48 Security > Content Filter > Filter

LABEL	DESCRIPTION
Enable URL Keyword Blocking	The NBG-417N 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 http://www.website.com/bad.html 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 Add 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 Delete to remove it. The keyword disappears from the text box after you click Apply .
Clear All	Click this button to remove all of the listed keywords.

Table 48 Security > Content Filter > Filter

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh

14.5 Technical Reference

The following section contains additional technical information about the NBG-417N features described in this chapter.

14.5.1 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

Domain Name or IP Address URL Checking

By default, the NBG-417N checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG-417N checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

Full Path URL Checking

Full path URL checking has the NBG-417N check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

File Name URL Checking

Filename URL checking has the NBG-417N check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

PART IV

Management

[Static Route \(143\)](#)

[Bandwidth Management \(147\)](#)

[Remote Management \(155\)](#)

[Universal Plug-and-Play \(UPnP\) \(159\)](#)

Static Route

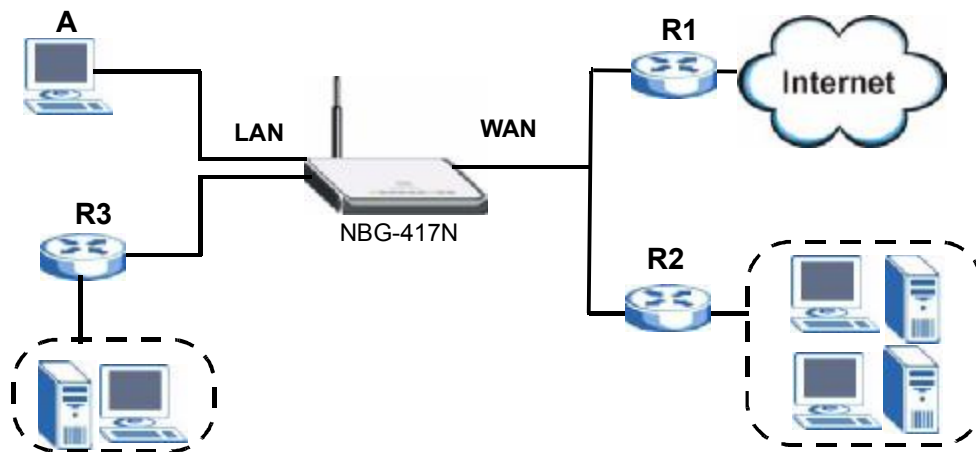
15.1 Overview

This chapter shows you how to configure static routes for your NBG-417N.

The NBG-417N usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the NBG-417N send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the NBG-417N's LAN interface. The NBG-417N routes most traffic from **A** to the Internet through the NBG-417N's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 73 Example of Static Routing Topology



15.2 What You Can Do in the IP Static Route Screens

- Use the **IP Static Route** screen ([Section 15.3 on page 144](#)) to view existing static route rules.
- Use the **Static Route Setup** screen ([Section 15.3.1 on page 145](#)) to add or edit a static route rule.

15.3 IP Static Route Screen

Use this screen to view existing static route rules. Click **Management > Static Route** to open the **IP Static Route** screen. The following screen displays.

Figure 74 Management > Static Route > IP Static Route



#	Name	Active	Destination	Gateway	Modify
1	default		0.0.0.0	172.23.37.254	
2					
3					
4					
5					
6					
7					
8					

The following table describes the labels in this screen.

Table 49 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
#	This is the index number of an individual static route. The first entry is for the default route and not editable.
Name	This is the name that describes or identifies this route.
Active	This icon is turned on when this static route is active. Click the Edit icon under Modify and select the Active checkbox in the Static Route Setup screen to enable the static route. Clear the checkbox to disable this static route without having to delete the entry.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.

Table 49 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your NBG-417N that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG-417N; over the WAN, the gateway must be the IP address of one of the remote nodes.
Modify	Click the Edit icon to open the static route setup screen. Modify a static route or create a new static route in the Static Route Setup screen. Click the Remove icon to delete a static route.

15.3.1 Static Route Setup Screen

To edit a static route, click the edit icon under **Modify**. The following screen displays. Fill in the required information for each static route.

Figure 75 Management > Static Route > IP Static Route: Static Route Setup

The following table describes the labels in this screen.

Table 50 Management > Static Route > IP Static Route: Static Route Setup

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your NBG-417N that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG-417N; over the WAN, the gateway must be the IP address of one of the Remote Nodes.

Table 50 Management > Static Route > IP Static Route: Static Route Setup

LABEL	DESCRIPTION
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click Apply to save your changes back to the NBG-417N.
Cancel	Click Cancel to return to the previous screen and not save your changes.

Bandwidth Management

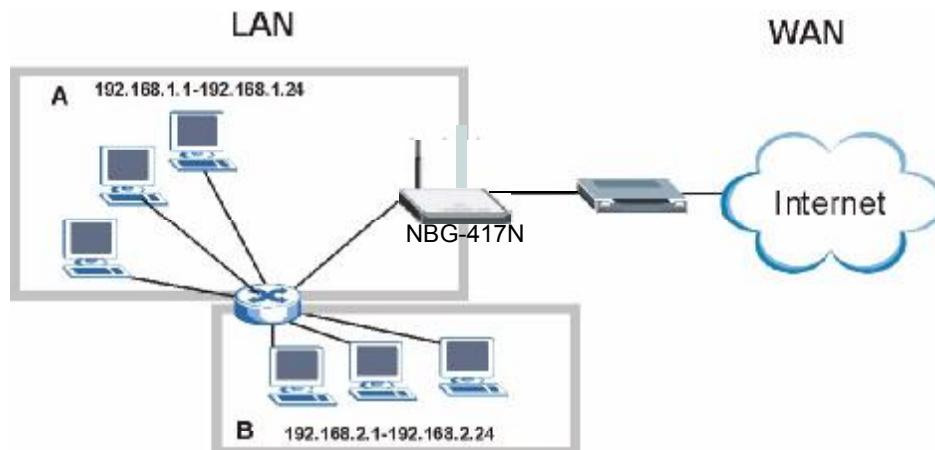
16.1 Overview

This chapter contains information about configuring bandwidth management, editing rules and viewing the NBG-417N's bandwidth management logs.

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example). You can also create bandwidth classes based on subnets. The following figure shows LAN subnets. You could configure one bandwidth class for subnet **A** and another for subnet **B**.

Figure 76 Subnet-based Bandwidth Management Example



16.2 What You Can Do in the Bandwidth Management Screen

- Use the **General** screen ([Section 16.4 on page 148](#)) to enable bandwidth management and assign bandwidth values.

- Use the **Advanced** screen ([Section 16.5 on page 150](#)) to configure bandwidth managements rule for the pre-defined service, other applications and/or subnets.

16.3 What You Need To Know About Bandwidth Management

The NBG-417N applies bandwidth management to traffic that it forwards out through an interface. The NBG-417N does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

- The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN, WAN to WAN / NBG-417N) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.
- The sum of the bandwidth allotments that apply to the LAN port (WAN to LAN, WLAN to LAN, LAN to LAN / NBG-417N) must be less than or equal to 100,000 kbps (you cannot configure the bandwidth budget for the LAN port).
- The sum of the bandwidth allotments that apply to the WLAN port (LAN to WLAN, WAN to WLAN, WLAN to WLAN / NBG-417N) must be less than or equal to 54,000 kbps (you cannot configure the bandwidth budget for the WLAN port).

16.4 Bandwidth Management General Configuration

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

Figure 77 Management > Bandwidth MGMT > General



The screenshot shows a web interface for configuring bandwidth management. At the top, there are two tabs: 'General' (which is active) and 'Advanced'. Below the tabs is a section titled 'Service Management'. Inside this section, there is a label 'Bandwidth Management Type' followed by a dropdown menu currently showing 'Disable'. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 51 Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
Enable Bandwidth Management	<p>This field allows you to have NBG-417N 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> <p>Select Priority Queue to allocate bandwidth based on the pre-defined priority assigned to an application.</p> <p>Select Bandwidth Allocation allocate specific amounts of bandwidth to specific applications and/or subnets.</p> <p>Select Disable if you do not want to use this feature.</p>
Apply	Click Apply to save your customized settings.
Reset	Click Reset to begin configuring this screen afresh.

16.5 Bandwidth Management Advanced Configuration

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

Figure 78 Management > Bandwidth MGMT > Advanced

The following table describes the labels in this screen.

Table 52 Management > Bandwidth MGMT > Advanced

LABEL	DESCRIPTION
Unlimited Priority Queue	
Local IP Address	Enter the IP address of the computer for which you want to allot the highest bandwidth priority.
Priority Queue	Use this table to allocate specific amounts of bandwidth based on the pre-defined service.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG-417N apply this bandwidth management rule.

Table 52 Management > Bandwidth MGMT > Advanced (continued)

LABEL	DESCRIPTION
Service	This is the name of the service.
Priority	Select a priority from the drop down list box. Choose High or Low .
Specific Port	This displays the port/s assigned to the service. You can also specify the port/s to services you want to allocate bandwidth for. Choose either Both , TCP or UDP in the drop-down menu and enter the port or range of ports in the provided boxes.
Bandwidth Allocation	Use this table to allocate specific amounts of bandwidth to specific applications and/or subnets.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG-417N apply this bandwidth management rule.
LAN IP Range	This displays the range of IP addresses for which the bandwidth management rule applies.
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. To LAN applies bandwidth management to traffic that the NBG-417N forwards to the LAN. To WAN applies bandwidth management to traffic that the NBG-417N forwards to the WAN. Both applies bandwidth management to traffic that the NBG-417N forwards to both the LAN and the WAN.
Port Range	This displays the range of ports for which the bandwidth management rule applies.
Policy	This displays either Max (maximum) or Min (minimum) and refers to the maximum or minimum bandwidth allowed for the rule in kilobits per second in the field below.
Rate	This is the maximum or minimum bandwidth allowed (refer to the field above) for the rule in kilobits per second.
Modify	Click the Edit icon to open the Rule Configuration screen. Modify an existing rule or create a new rule in the Rule Configuration screen. See Section 16.5.1 on page 152 for more information. Click the Remove icon to delete a rule.
Apply	Click Apply to save your customized settings.
Reset	Click Reset to begin configuring this screen afresh.

16.5.1 Rule Configuration: User Defined Service Rule Configuration

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

Figure 79 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration

The following table describes the labels in this screen

Table 53 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration

LABEL	DESCRIPTION
Active	Select this check box to turn on this bandwidth management rule.
Direction	Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Select To LAN applies bandwidth management to traffic that the NBG-417N forwards to the LAN. Select To WAN applies bandwidth management to traffic that the NBG-417N forwards to the WAN. Select Both applies bandwidth management to traffic that the NBG-417N forwards to both the LAN and the WAN.
LAN IP Range	Specify the range of IP addresses for which the bandwidth management rule applies.
Protocol	Select the protocol (TCP, UDP, SMTP, HTTP, POP3, FTP or ALL) for which the bandwidth management rule applies.
Port Range	Enter the range of ports for which the bandwidth management rule applies.
Policy	Select Max or Min and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second in the field below.
Rate (bps)	Enter the maximum or minimum bandwidth allowed (refer to the field above) for the rule in bits per second.

LABEL	DESCRIPTION
OK	Click OK to save your customized settings.
Cancel	Click Cancel to exit this screen without saving.

16.6 Technical References

The following section contains additional technical information about the NBG-417N features described in this chapter.

16.6.1 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 54 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

16.6.2 Bandwidth Management Priorities

The following table describes the priorities that you can apply to traffic that the NBG-417N forwards out through an interface.

Table 55 Bandwidth Management Priorities

PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED.	
High	Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).
Low	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.

16.6.3 Predefined Bandwidth Management Services

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

Table 56 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. FTP uses port number 21.
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. WWW uses port 80.
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. Telnet uses port 23.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 SMTP - port 25
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files using ports 6881 to 6889. 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. One example is Microsoft's Xbox Live, which uses port 3074.

16.6.4 Services and Port Numbers

See [Appendix F on page 257](#) for commonly used services and port numbers.

Remote Management

17.1 Overview

This chapter provides information on the Remote Management screens.

Remote management allows you to determine which services/protocols can access which NBG-417N interface (if any) from which computers.

You may manage your NBG-417N from a remote location via:

- LAN only
- LAN and WAN

Note: When you configure remote management to allow management from the **LAN & WAN** in the options above, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

17.2 What You Can Do in the Remote Management Screens

Use the **WWW** screen ([Section 17.4 on page 157](#)) to change your NBG-417N's World Wide Web settings.

17.3 What You Need To Know About Remote Management

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field. You may only have one remote management session running at a time.

17.3.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 You have disabled that service in one of the remote management screens.
- 2 The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the NBG-417N will disconnect the session immediately.
- 3 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- 4 There is a firewall rule that blocks it.

17.3.2 Remote Management and NAT

When NAT is enabled:

- Use the NBG-417N's WAN IP address when configuring from the WAN.
- Use the NBG-417N's LAN IP address when configuring from the LAN.

17.3.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG-417N 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

17.4 WWW Screen

To change your NBG-417N's World Wide Web settings, click **Management** > **Remote MGMT** to display the **WWW** screen.

Figure 80 Management > Remote MGMT > WWW

The following table describes the labels in this screen

Table 57 Management > Remote MGMT > 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-417N using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NBG-417N using this service. Select All to allow any computer to access the NBG-417N using this service. Choose Selected to just allow the computer with the IP address that you specify to access the NBG-417N using this service. Note: This only applies on WAN IP.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Universal Plug-and-Play (UPnP)

18.1 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.

18.2 What You Can Do in the UPnP Screen

Use the **UPnP** screen ([Section 18.4 on page 161](#)) to enable UPnP on the NBG-417N.

18.3 What You Need to Know About UPnP

How do I know if I'm using UPnP?

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.

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.

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-417N 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.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See the following sections for examples of installing and using UPnP.

18.4 UPnP Screen

Use this screen to enable UPnP. Click the **Management > UPnP** to open the following screen.

Figure 81 Management > UPnP > General

General

UPnP Setup

Device Name : ZyXEL NBG-417N Internet Sharing Gateway

Enable the Universal Plug and Play (UPnP) Feature

Allow users to make port forwarding changes through UPnP

Note:

1. For UPnP to function normally, the [HTTP](#) service must be available for LAN computers using UPnP.

2. For [WPS](#) to function normally, the UPnP service must be available.

Apply Reset

The following table describes the labels in this screen.

Table 58 Management > UPnP > General

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-417N's IP address (although you must still enter the password to access the Web Configurator).
Allow users to make port forwarding changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the NBG-417N so that they can communicate through the NBG-417N, for example by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click Apply to save the setting to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

18.5 Technical Reference

The following section contains additional technical information about the NBG-417N features described in this chapter.

18.5.1 Installing UPnP in Windows Example

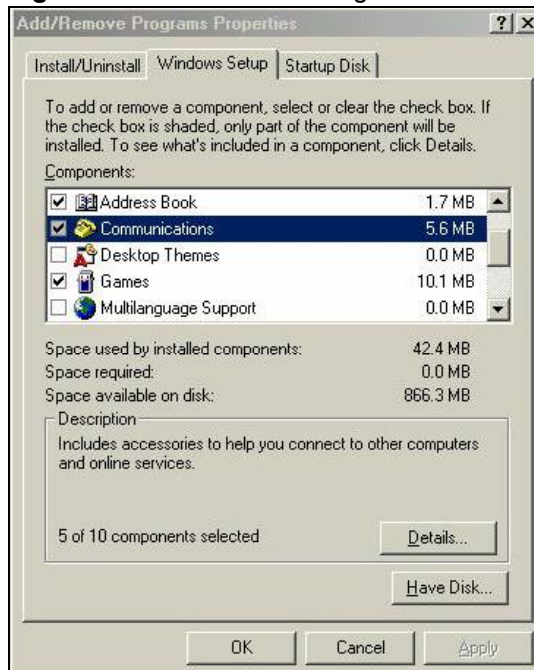
This section shows how to install UPnP in Windows Me and Windows XP.

18.5.1.1 Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

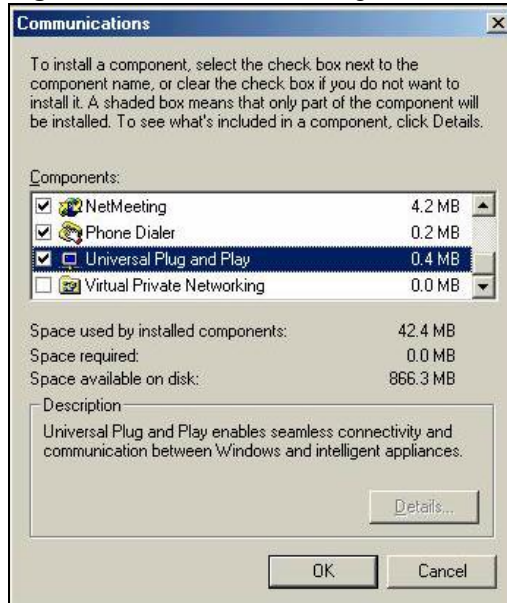
- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 82 Add/Remove Programs: Windows Setup: Communication



- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 83 Add/Remove Programs: Windows Setup: Communication: Components



- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

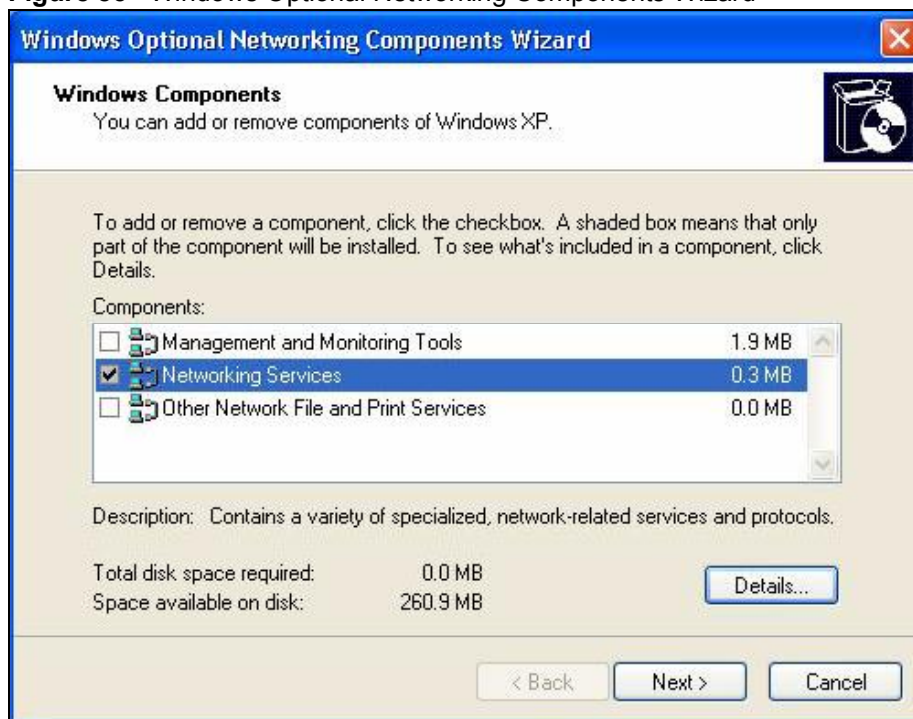
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**

Figure 84 Network Connections



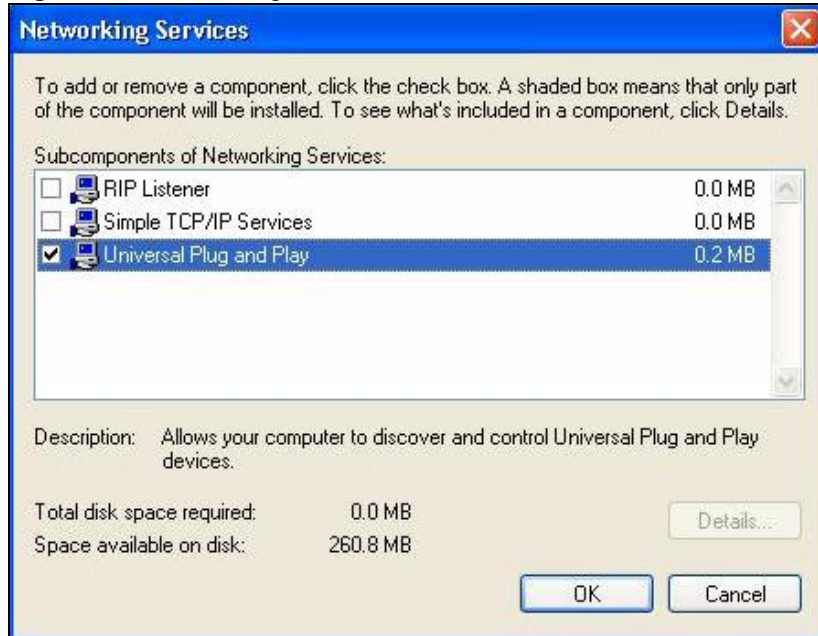
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 85 Windows Optional Networking Components Wizard



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 86 Networking Services



- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

18.5.1.2 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-417N.

Make sure the computer is connected to a LAN port of the NBG-417N. Turn on your computer and the NBG-417N.

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 87 Network Connections



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

Figure 88 Internet Connection Properties



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

Figure 89 Internet Connection Properties: Advanced Settings

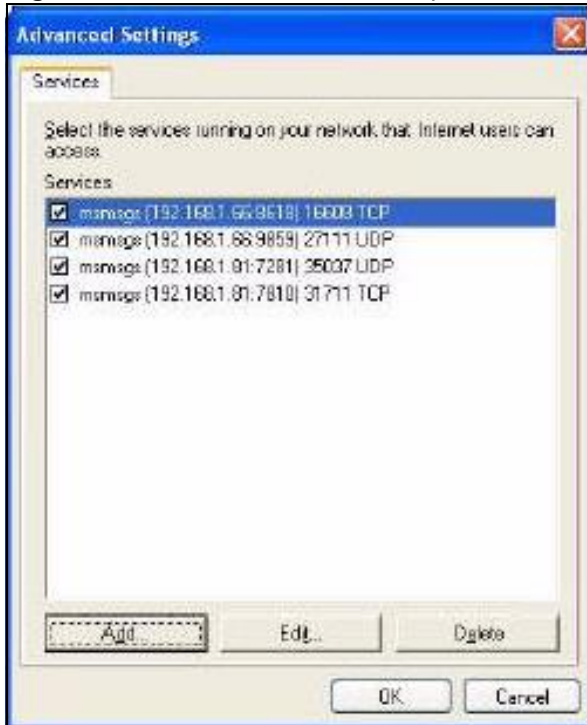
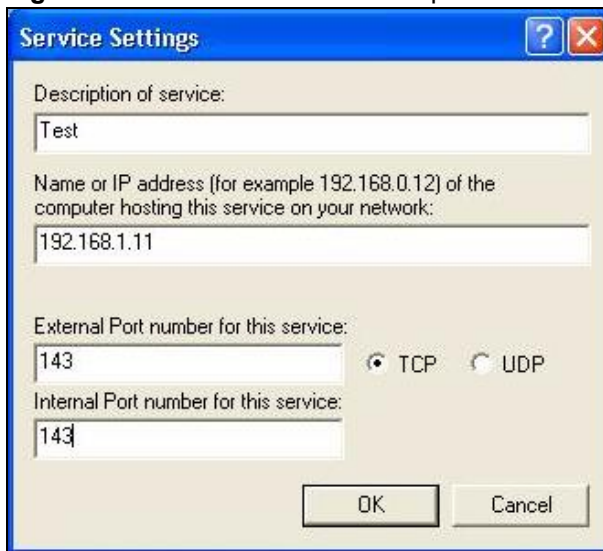


Figure 90 Internet Connection Properties: Advanced Settings: Add



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

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

Figure 91 System Tray Icon



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

Figure 92 Internet Connection Status



Web Configurator Easy Access

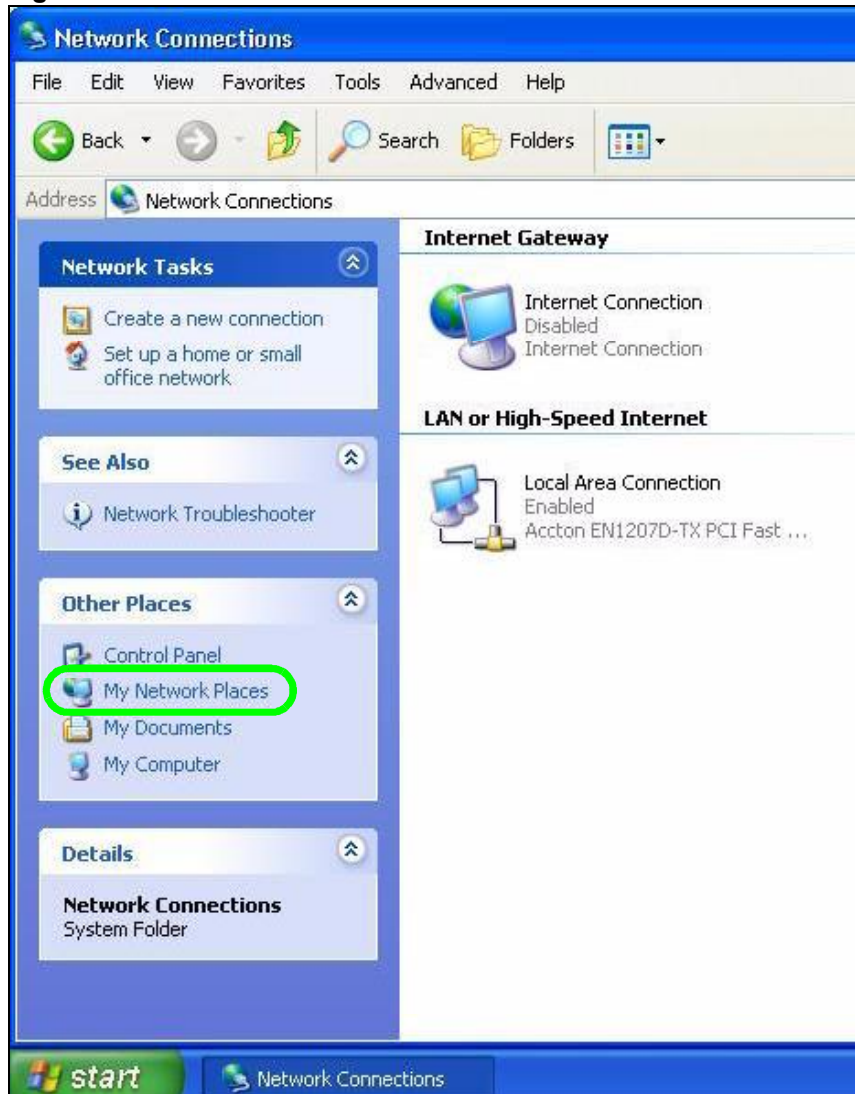
With UPnP, you can access the web-based configurator on the NBG-417N without finding out the IP address of the NBG-417N first. This comes helpful if you do not know the IP address of the NBG-417N.

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 93 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-417N and select **Invoke**. The Web Configurator login screen displays.

Figure 94 Network Connections: My Network Places



- 6 Right-click on the icon for your NBG-417N and select **Properties**. A properties window displays with basic information about the NBG-417N.

Figure 95 Network Connections: My Network Places: Properties: Example



PART V

Maintenance and Troubleshooting

[System \(175\)](#)

[Logs \(181\)](#)

[Tools \(183\)](#)

[Sys OP Mode \(189\)](#)

[Language \(193\)](#)

[Troubleshooting \(195\)](#)

19

System

19.1 Overview

This chapter provides information on the **System** screens.

See the chapter about wizard setup for more information on the next few screens.

19.2 What You Can Do in the System Screens

- Use the **General** screen ([Section 19.3 on page 175](#)) to enter a name to identify the NBG-417N in the network and set the password.
- Use the **Time Setting** screen ([Section 19.4 on page 177](#)) to change your NBG-417N's time and date.

19.3 System General Screen

Use this screen to enter a name to identify the NBG-417N in the network and set the password. Click **Maintenance > System**. The following screen displays.

Figure 96 Maintenance > System > General

The screenshot shows a web interface for system configuration. At the top, there are two tabs: 'General' (selected) and 'Time Setting'. Below the tabs is a 'System Setup' section with three input fields: 'System Name' containing 'NBG-417N', 'Domain Name' containing 'zyxel.com', and 'Administrator Inactivity Timer' set to '0' with a note '(minutes, 0 means no timeout)'. Below this is a 'Password Setup' section with three input fields: 'Old Password', 'New Password', and 'Retype to Confirm', all containing '****'. At the bottom of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 59 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	<p>System Name is a unique name to identify the NBG-417N in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name).</p> <p>This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.</p>
Domain Name	<p>Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.</p> <p>The domain name entered by you is given priority over the ISP assigned domain name.</p>
Administrator Inactivity Timer	<p>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).</p>
Password Setup	<p>Change your NBG-417N's password (recommended) using the fields as shown.</p>
Old Password	<p>Type the default password or the existing password you use to access the system in this field.</p>
New Password	<p>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.</p>
Retype to Confirm	<p>Type the new password again in this field.</p>
Apply	<p>Click Apply to save your changes back to the NBG-417N.</p>
Reset	<p>Click Reset to begin configuring this screen afresh.</p>

19.4 Time Setting Screen

To change your NBG-417N's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the NBG-417N's time based on your local time zone.

Figure 97 Maintenance > System > Time Setting

The following table describes the labels in this screen.

Table 60 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG-417N. Each time you reload this page, the NBG-417N synchronizes the time with the time server.
Current Date	This field displays the date of your NBG-417N. Each time you reload this page, the NBG-417N synchronizes the date with the time server.
Time and Date Setup	
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.

Table 60 Maintenance > System > Time Setting

LABEL	DESCRIPTION
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 Time and Date Setup to Manual , enter the new time in this field and then click Apply .
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 Time and Date Setup to Manual , enter the new date in this field and then click Apply .
Get from Time Server	Select this radio button to have the NBG-417N get the time and date from the time server you specified below.
Auto	Select Auto to have the NBG-417N automatically search for an available time server and synchronize the date and time with the time server after you click Apply .
User Defined Time Server Address	Select User Defined Time Server Address 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.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Daylight Savings . The o'clock field uses the 24 hour format. Here are a couple of examples: 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 First, Sunday, April and type 2 in the o'clock field. 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 Last, Sunday, March . The time you type in the o'clock 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).

Table 60 Maintenance > System > Time Setting

LABEL	DESCRIPTION
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Daylight Savings. The o'clock 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 Last, Sunday, October and type 2 in the o'clock 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 Last, Sunday, October. The time you type in the o'clock 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 Apply to save your changes back to the NBG-417N.
Reset	Click Reset to begin configuring this screen afresh.

20

Logs

20.1 Overview

This chapter contains information about configuring general log settings and viewing the NBG-417N's logs. Refer to the appendices for example log message explanations.

The Web Configurator allows you to look at all of the NBG-417N's logs in one location.

20.2 What You Can Do in the Log Screens

Use the **View Log** screen ([Section 20.4 on page 182](#)) 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.

20.3 What You Need to Know About Logs

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.

20.4 View Log Screen

Use the **View Log** screen to see the logged messages for the NBG-417N. 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 > Logs** to open the **View Log** screen.

Figure 98 Maintenance > Logs > View Log

#	Time	Message
1	Dec 19 12:53:46	NTP, Local time=2008/12/19 12:53:46
2	Dec 19 12:53:46	NTP, Daylight saving status: Disable
3	Dec 19 12:53:46	NTP, Time zone = (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei
4	Dec 19 11:53:43	NTP, Local time=2008/12/19 11:53:43
5	Dec 19 11:53:43	NTP, Daylight saving status: Disable
6	Dec 19 11:53:43	NTP, Time zone = (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei
7	Dec 19 10:55:30	NET, start Firewall
8	Dec 19 10:55:30	NET, start NAT
9	Dec 19 10:55:30	NET, start

The following table describes the labels in this screen.

Table 61 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.
#	This is the index number of the log entry.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the NBG-417N's time and date.
Message	This field states the reason for the log.

21

Tools

21.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG-417N.

21.2 What You Can Do in the Tools Screen

- Use the **Firmware** screen ([Section 21.3 on page 183](#)) to upload firmware to your NBG-417N.
- Use the **Configuration** screen ([Section 21.4 on page 186](#)) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use the **Restart** screen ([Section 21.5 on page 188](#)) to have the NBG-417N reboot.

21.3 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "NBG-417N.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 > Tools**. Follow the instructions in this screen to upload firmware to your NBG-417N.

Figure 99 Maintenance > Tools > Firmware

The following table describes the labels in this screen.

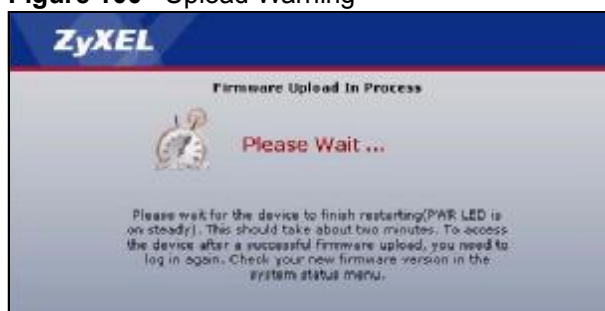
Table 62 Maintenance > Tools > Firmware

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

Note: Do not turn off the NBG-417N while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG-417N again.

Figure 100 Upload Warning



The NBG-417N automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 101 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, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 102 Upload Error Message



21.4 Configuration Screen

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 103 Maintenance > Tools > Configuration

The screenshot shows a web interface with three tabs: 'Firmware', 'Configuration' (selected), and 'Restart'. Below the tabs are three sections:

- Backup Configuration:** A heading followed by the text 'Click **Backup** to save the current configuration of your system to your computer.' and a 'Backup' button.
- Restore Configuration:** A heading followed by the text 'To restore a previously saved configuration file to your system, browse to the location of the configuration file and click **Upload**.' Below this is a 'File Path:' label, an empty text input field, and a 'Browse...' button. Below the input field is an 'Upload' button.
- Back to Factory Defaults:** A heading followed by the text 'Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the' and a list of defaults:
 - Password will be 1234
 - LAN IP address will be 192.168.1.1
 - DHCP will be reset to serverBelow the list is a 'Reset' button.

21.4.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG-417N's current configuration to a file on your computer. Once your NBG-417N 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.

Click **Backup** to save the NBG-417N's current configuration to your computer.

21.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG-417N.

Table 63 Maintenance Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse... to find it.
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin the upload process.

Note: Do not turn off the NBG-417N while configuration file upload is in progress

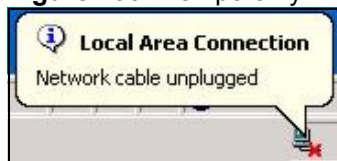
After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG-417N again.

Figure 104 Configuration Restore Successful



The NBG-417N automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 105 Temporarily Disconnected



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-417N IP address (192.168.1.1). See [Appendix D on page 227](#) for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 106 Configuration Restore Error



21.4.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG-417N to its factory defaults.

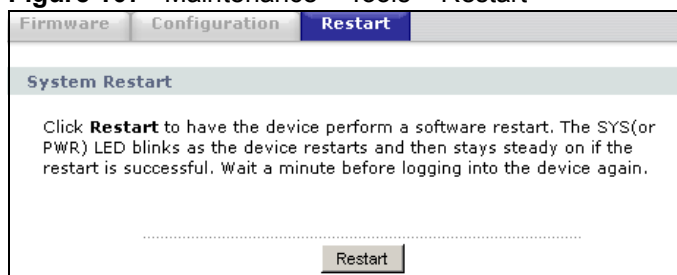
You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG-417N. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

21.5 Restart Screen

System restart allows you to reboot the NBG-417N without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the NBG-417N reboot. This does not affect the NBG-417N's configuration.

Figure 107 Maintenance > Tools > Restart



Sys OP Mode

22.1 Overview

The **Sys OP Mode** (System Operation Mode) function lets you configure whether your NBG-417N is a router or AP. You can choose between **Router Mode** and **AP Mode** depending on your network topology and the features you require from your device. See [Section 1.1 on page 21](#) for more information on which mode to choose.

22.2 What You Can Do in the Sys OP Mode Screen

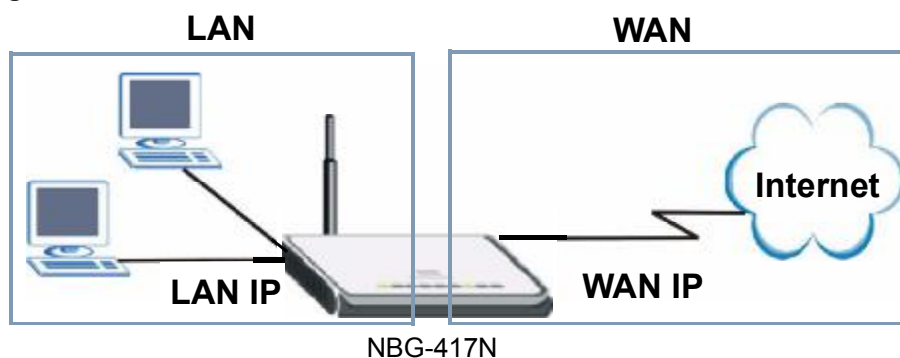
Use the General screen ([Section 22.4 on page 191](#)) to select how you connect to the Internet.

22.3 What You Need to Know About Sys OP Mode

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.

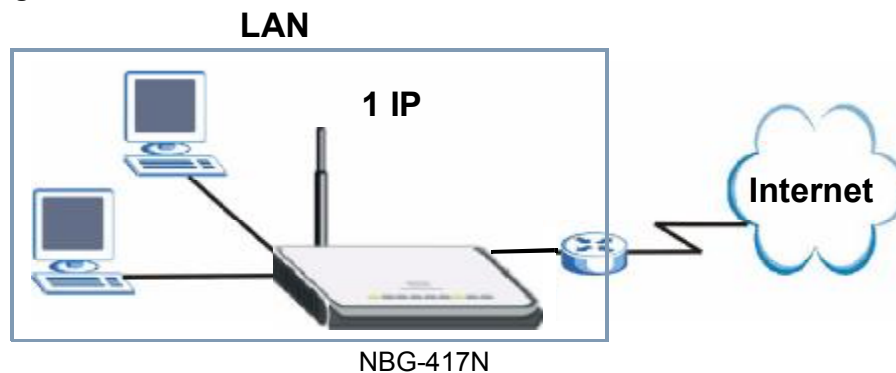
Figure 108 LAN and WAN IP Addresses in Router Mode



AP

An AP extends one network and so has just one IP address. All Ethernet ports on the AP have the same IP address. To connect to the Internet, another device, such as a router, is required.

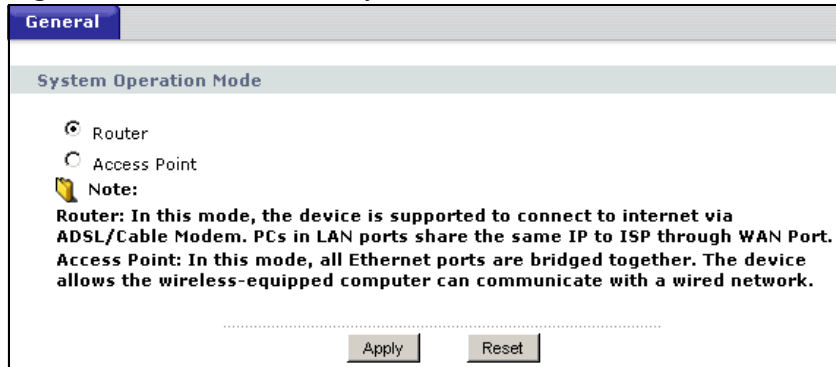
Figure 109 IP Address in AP Mode



22.4 General Screen

Use this screen to select how you connect to the Internet.

Figure 110 Maintenance > Sys OP Mode > General



If you select Router Mode, the following pop-up message window appears.

Figure 111 Maintenance > Sys Op Mode > General: Router



- In this mode there are both LAN and WAN ports. The LAN Ethernet and WAN Ethernet ports have different IP addresses.
- The DHCP server on your device is enabled and allocates IP addresses to other devices on your local network.
- The LAN IP address of the device on the local network is set to 192.168.1.1.
- You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

If you select Access Point the following pop-up message window appears.

Figure 112 Maintenance > Sys Op Mode > General: AP



- In **AP Mode** all Ethernet ports have the same IP address.
- All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port.

- The DHCP server on your device is disabled. In AP mode there must be a device with a DHCP server on your network such as a router or gateway which can allocate IP addresses.

The IP address of the device on the local network is set to 192.168.1.2.

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

Table 64 Maintenance > Sys OP Mode > General

LABEL	DESCRIPTION
System Operation Mode	
Router	Select Router 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.
Access Point	Select Access Point if your device bridges traffic between clients on the same network.
Apply	Click Apply to save your settings.
Reset	Click Reset to return your settings to the default (Router)

Note: If you select the incorrect System Operation Mode you cannot connect to the Internet.

Language

23.1 Language Screen

Use this screen to change the language for the Web Configurator display.

Click the language you prefer. The Web Configurator language changes after a while without restarting the NBG-417N.

Figure 113 Language



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-417N Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG-417N to Its Factory Defaults](#)
- [Wireless Router/AP Troubleshooting](#)

24.1 Power, Hardware Connections, and LEDs

The NBG-417N 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-417N.
- 2 Make sure the power adaptor or cord is connected to the NBG-417N 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-417N.
- 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-417N.
- 5 If the problem continues, contact the vendor.

24.2 NBG-417N Access and Login

I don't know the IP address of my NBG-417N.

- 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-417N 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-417N (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-417N'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-417N 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-417N to change all settings back to their default. This means your current settings are lost. See [Section 24.4 on page 200](#) in the **Troubleshooting** for information on resetting your NBG-417N.

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 24.4 on page 200](#).

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 7.3 on page 102](#)), 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-417N](#).
- 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 B on page 209](#).
- 4 Make sure your computer is in the same subnet as the NBG-417N. (If you know that there are routers between your computer and the NBG-417N, skip this step.)
 - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 7.3 on page 102](#).
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG-417N. See [Section 7.3 on page 102](#).
- 5 Reset the device to its factory defaults, and try to access the NBG-417N with the default IP address. See [Section 7.3 on page 102](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG-417N using another service, such as Telnet. If you can access the NBG-417N, check the remote management settings and firewall rules to find out why the NBG-417N does not respond to HTTP.
- 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-417N.

- 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 You cannot log in to the Web Configurator while someone is using Telnet to access the NBG-417N. Log out of the NBG-417N in the other session, or ask the person who is logged in to log out.
- 3 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- 4 Disconnect and re-connect the power adaptor or cord to the NBG-417N.
- 5 If this does not work, you have to reset the device to its factory defaults. See [Section 24.4 on page 200](#).

24.3 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-417N 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-417N), 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-417N.
- 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-417N 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-417N 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-417N.
- 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.

24.4 Resetting the NBG-417N to Its Factory Defaults

If you reset the NBG-417N, you lose all of the changes you have made. The NBG-417N 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-417N,

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the NBG-417N.
- 3 Press the **RESET** button for longer than five seconds to set the NBG-417N back to its factory-default configurations.

If the NBG-417N restarts automatically, wait for the NBG-417N to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG-417N does not restart automatically, disconnect and reconnect the NBG-417N's power. Then, follow the directions above again.

24.5 Wireless Router/AP Troubleshooting

I cannot access the NBG-417N or ping any computer from the WLAN (wireless AP or router).

- 1 Make sure the wireless LAN is enabled on the NBG-417N
- 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-417N.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG-417N.

- 5 Check that both the NBG-417N 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-417N.
 - 7 Make sure you allow the NBG-417N 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 D on page 227](#) for instructions on how to change your computer's IP address.

PART VI

Appendices and Index

Product Specifications (205)

Pop-up Windows, JavaScripts and Java
Permissions (209)

IP Addresses and Subnetting (217)

Setting up Your Computer's IP Address
(227)

Wireless LANs (245)

Services (257)

Legal Information (261)

Index (265)

Product Specifications

The following tables summarize the NBG-417N's hardware and firmware features.

Table 65 Hardware Features

Dimensions (W x D x H)	140 mm x 110 mm x 30 mm
Weight	190 g
Power Specification	Input: 120~240 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-417N a cost-effective and viable network solution. You can add up to four computers to the NBG-417N 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-417N 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-417N 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.
Antenna	The NBG-417N is equipped with three 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 66 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	Wireless LAN: ZyXEL Wireless LAN when WPS enabled: ZyXEL WPS
Default Wireless IP Address	Wireless LAN: Same as LAN (192.168.1.1)
Default Wireless Subnet Mask	Wireless LAN: Same as LAN (255.255.255.0)
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-417N.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the NBG-417N wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The NBG-417N 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-417N. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the NBG-417N's configuration and put it back on the NBG-417N 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-417N 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 66 Firmware Features

FEATURE	DESCRIPTION
Content Filter	The NBG-417N 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-417N 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-417N.
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-417N. 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-417N 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, www.zyxel.com 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-417N 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-417N supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The NBG-417N can communicate with other UPnP enabled devices in a network.

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

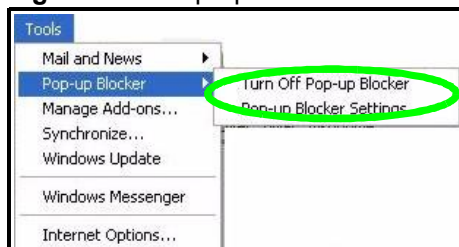
You may have to disable pop-up blocking to log into your device.

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**.

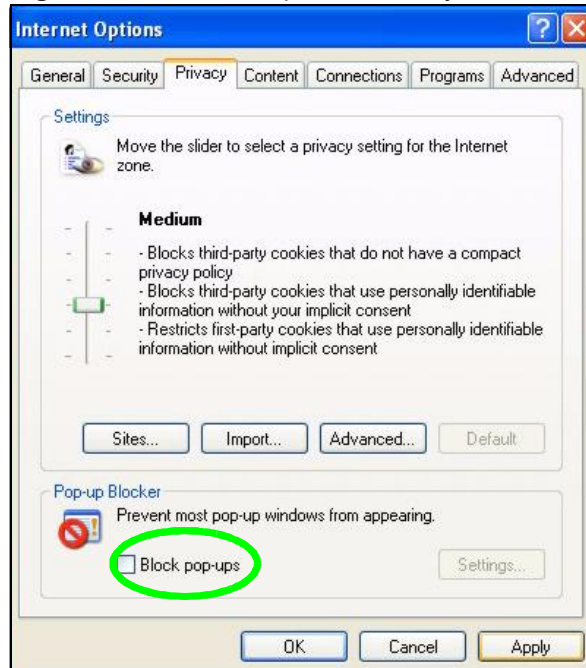
Figure 114 Pop-up Blocker



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 115 Internet Options: Privacy



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

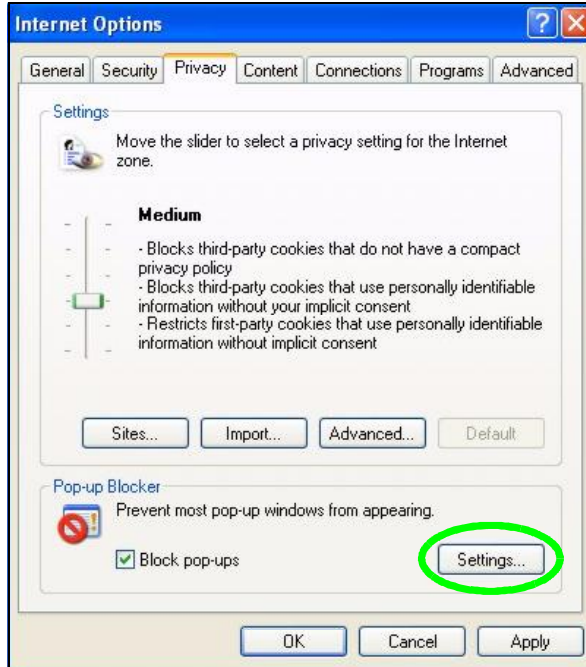
Enable pop-up Blockers with Exceptions

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.

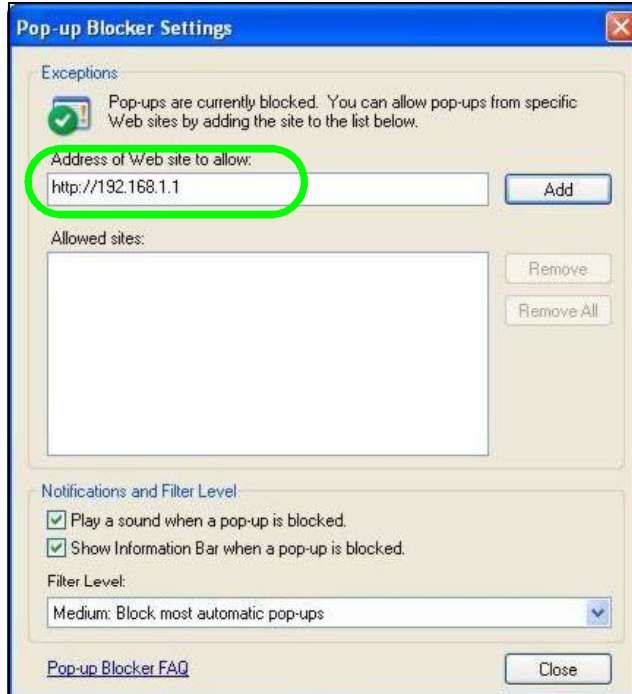
Figure 116 Internet Options: Privacy



- 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 117 Pop-up Blocker Settings



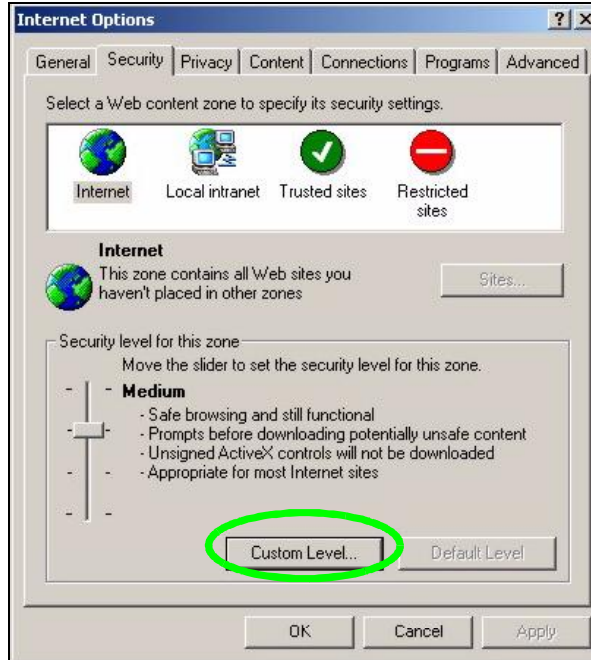
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

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.

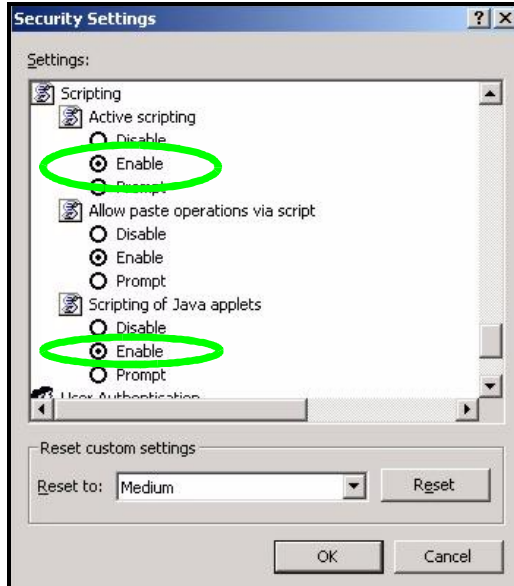
Figure 118 Internet Options: Security



- 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 119 Security Settings - Java Scripting

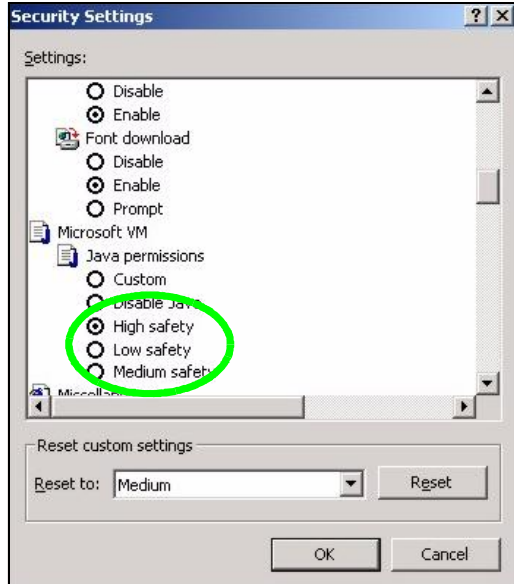


Java Permissions

- 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 120 Security Settings - Java

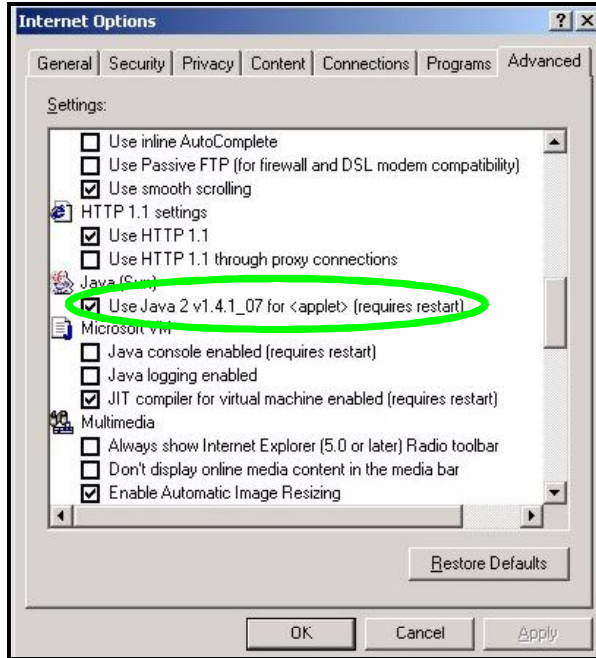


JAVA (Sun)

- 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 121 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.

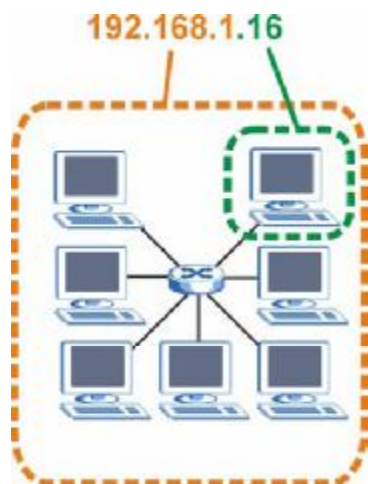
Structure

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 122 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 67 Subnet Mask - Identifying Network Number

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

Table 67 Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
Network Number	11000000	10101000	00000001	
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 68 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 69 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 70 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

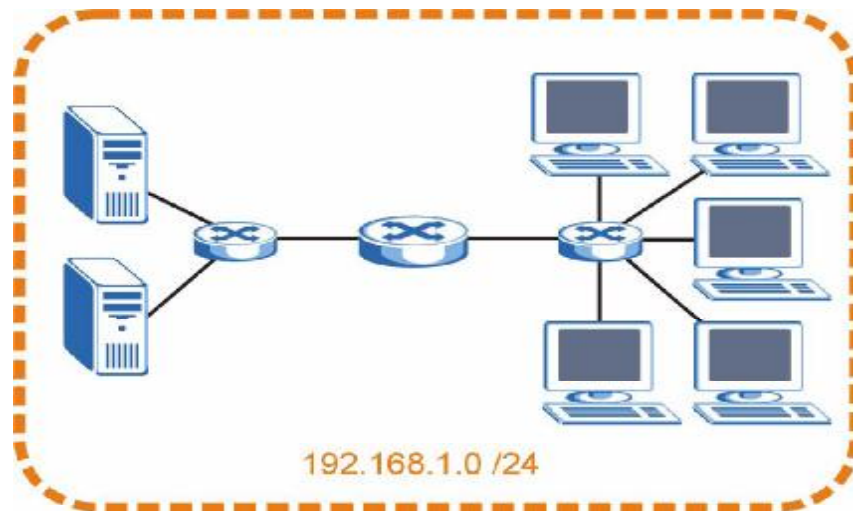
Subnetting

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 123 Subnetting Example: Before Subnetting

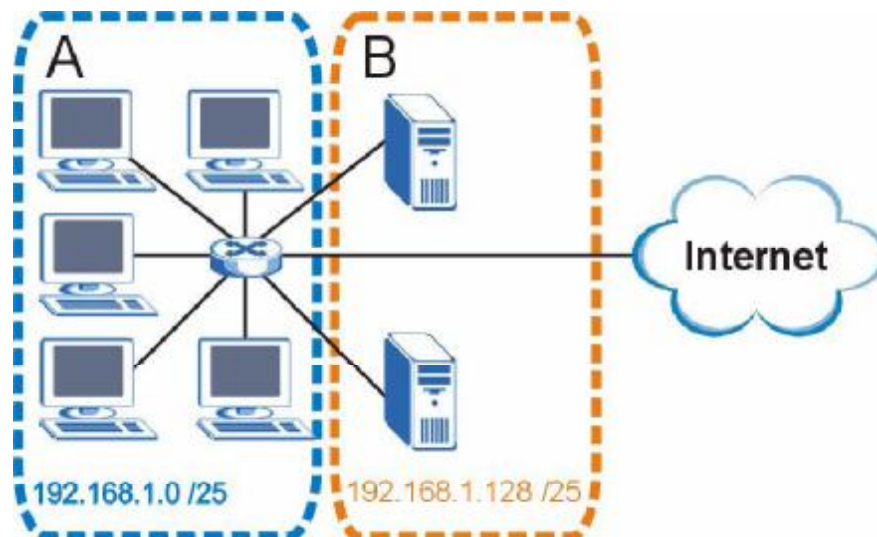


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 124 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 71 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 72 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 73 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 74 Subnet 4

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

Table 74 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 75 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 76 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 77 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-417N.

Once you have decided on the network number, pick an IP address for your NBG-417N 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-417N 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-417N 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*.

D

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.

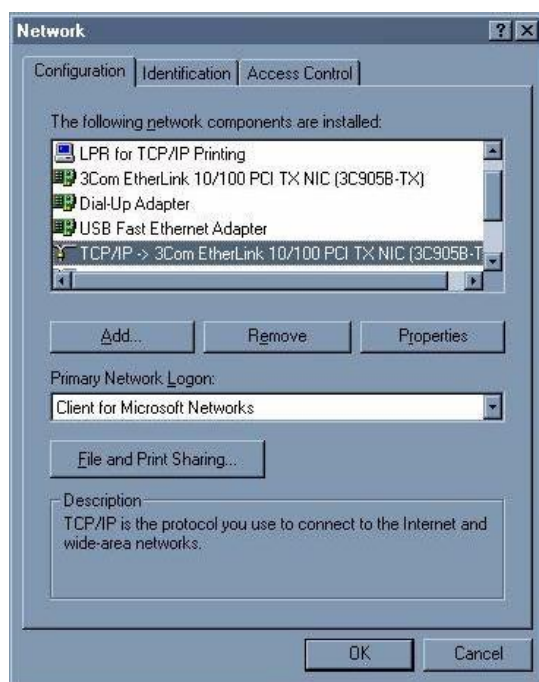
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 125 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**.

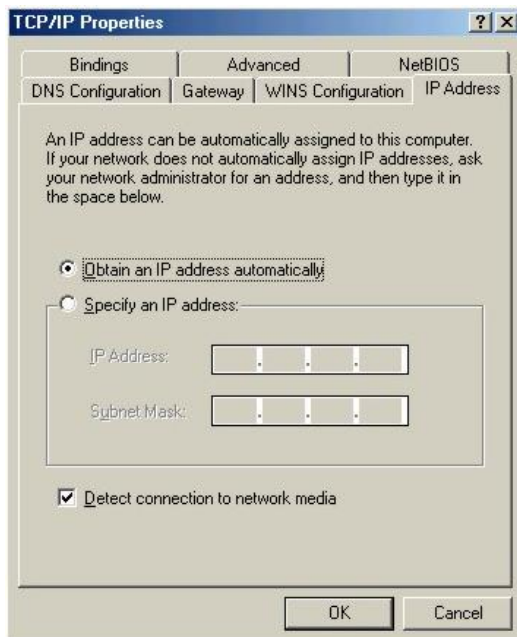
If you need Client for Microsoft Networks:

- 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

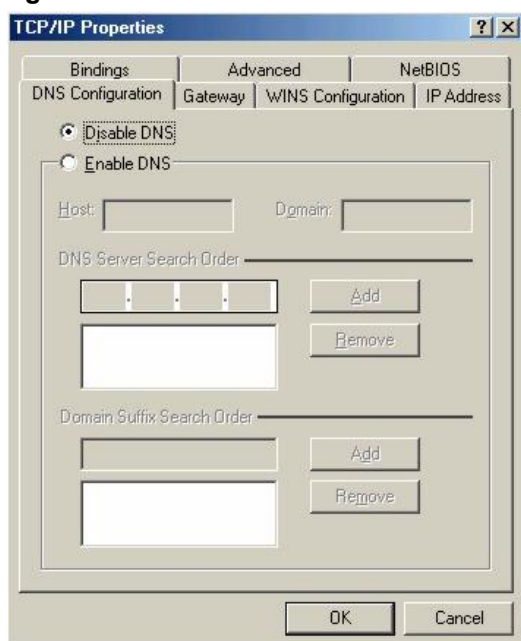
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 126 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 127 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.

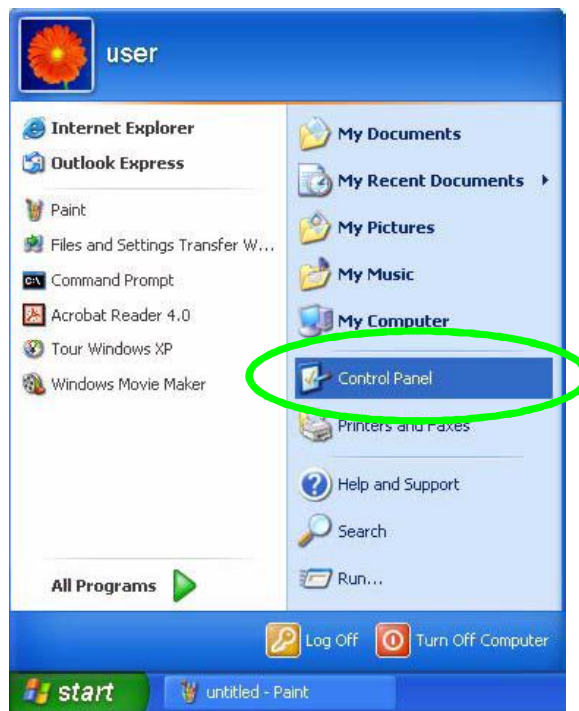
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

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 128 Windows XP: Start Menu



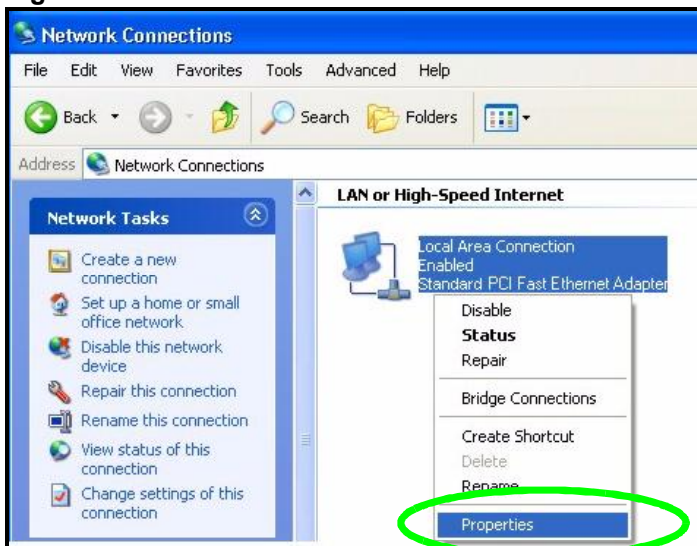
- 2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

Figure 129 Windows XP: Control Panel



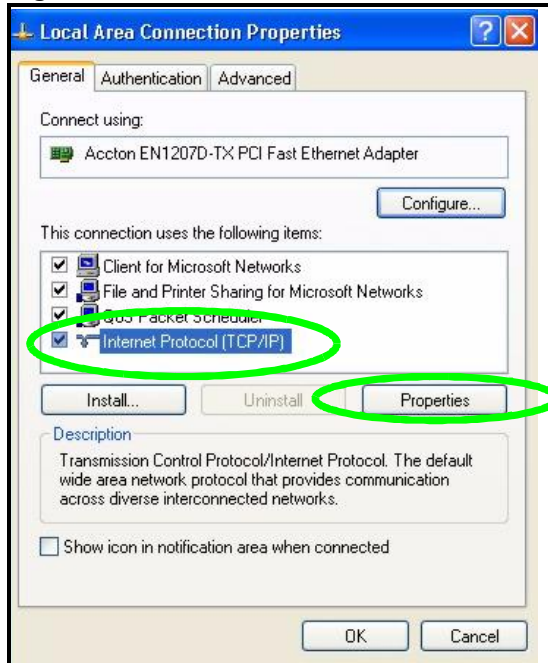
- 3 Right-click **Local Area Connection** and then click **Properties**.

Figure 130 Windows XP: Control Panel: Network Connections: Properties



- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

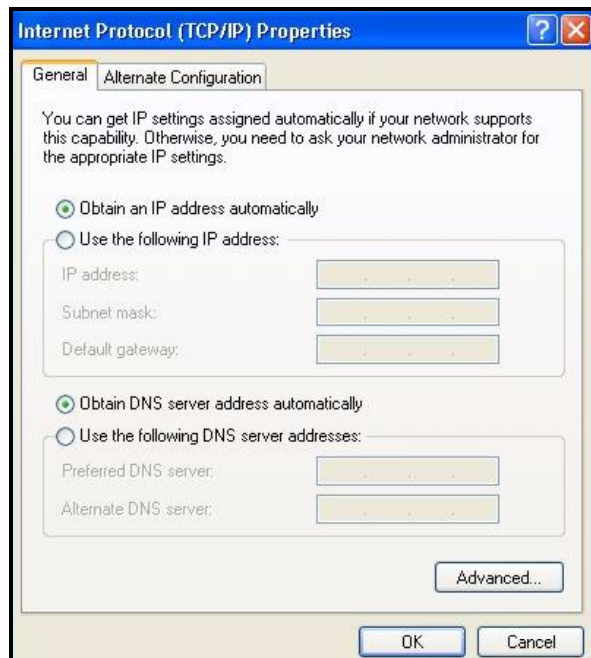
Figure 131 Windows XP: Local Area Connection Properties



- 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 132 Windows XP: Internet Protocol (TCP/IP) Properties



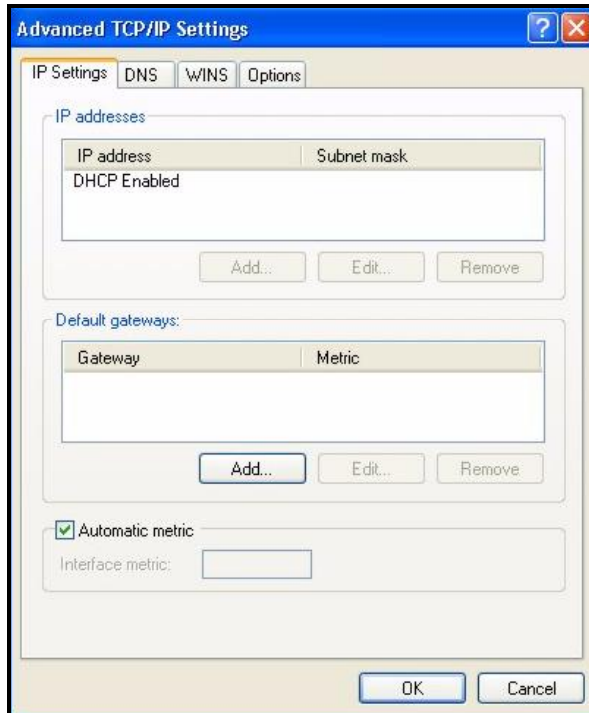
- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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.

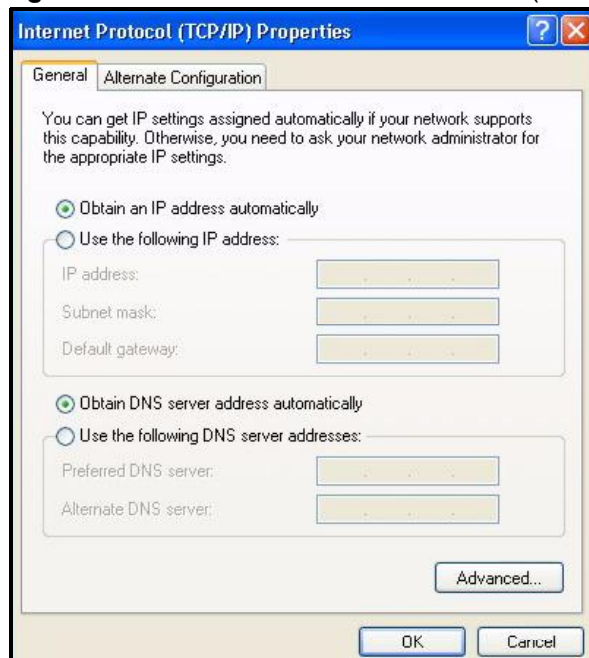
Figure 133 Windows XP: Advanced TCP/IP Properties



- 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 134 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).

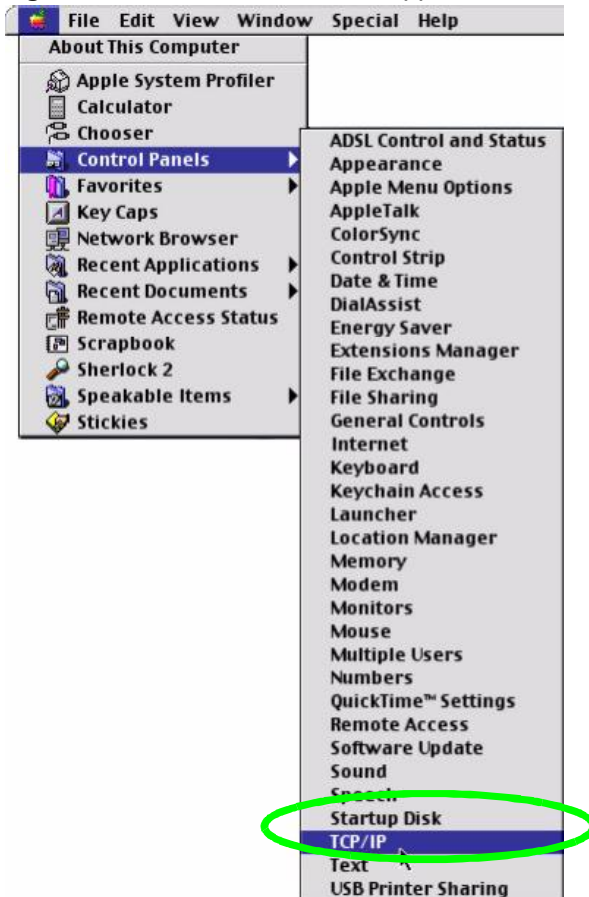
Verifying Settings

- 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

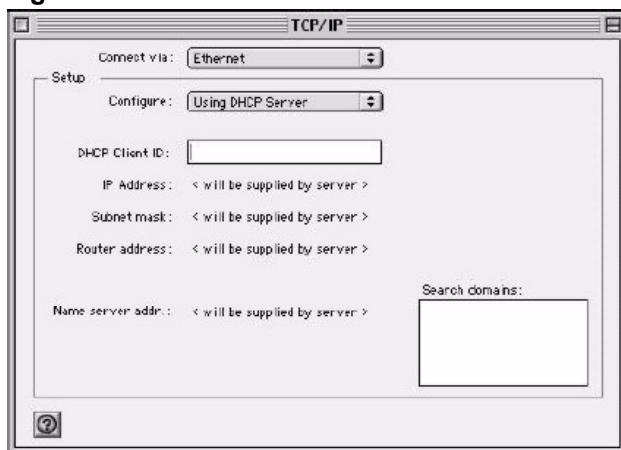
- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 135 Macintosh OS 8/9: Apple Menu



- 2 Select **Ethernet built-in** from the **Connect via** list.

Figure 136 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).

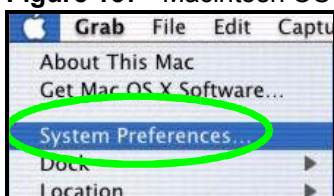
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

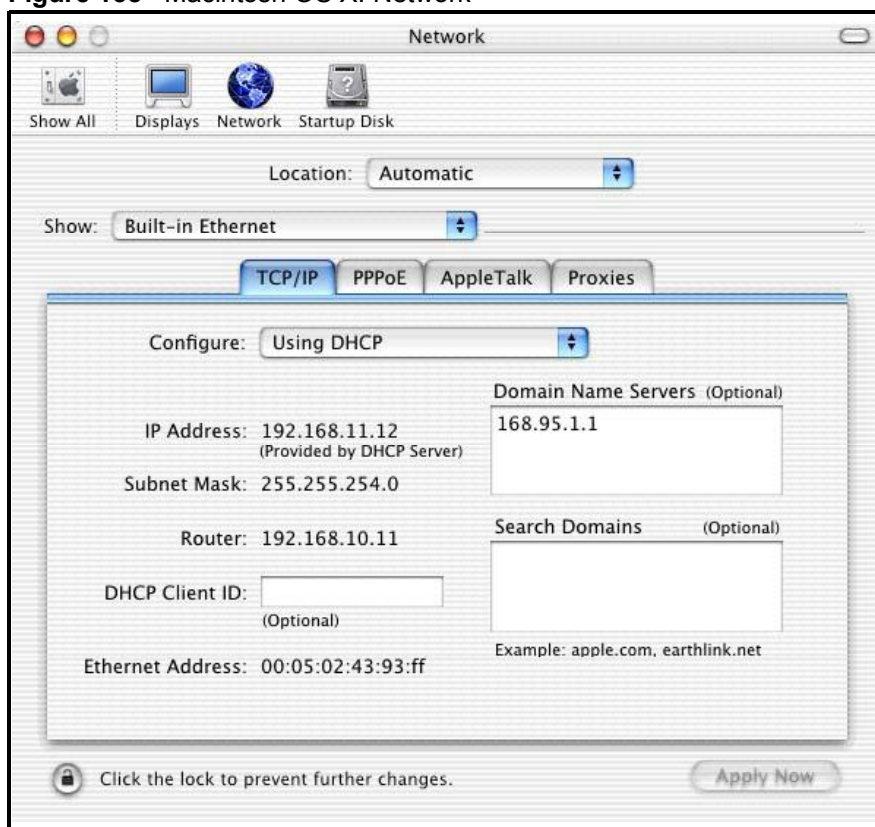
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 137 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 138 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 139 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 140 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 141 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 142 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 143 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 144 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 145 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 146 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]
```

24.5.1 Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 147 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 148 Peer-to-Peer Communication in an Ad-hoc Network



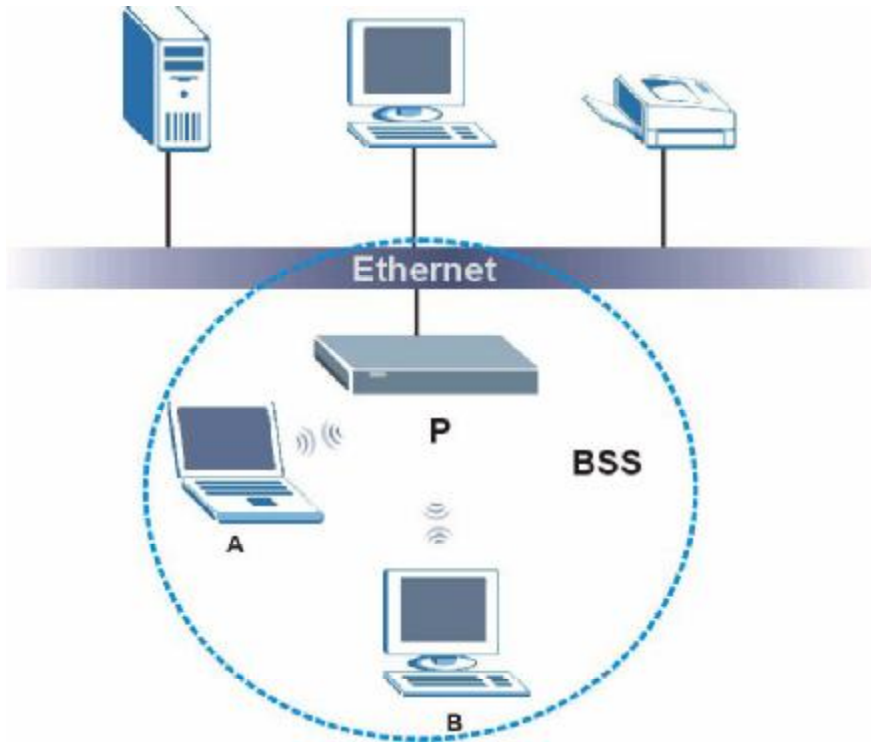
BSS

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 149 Basic Service Set



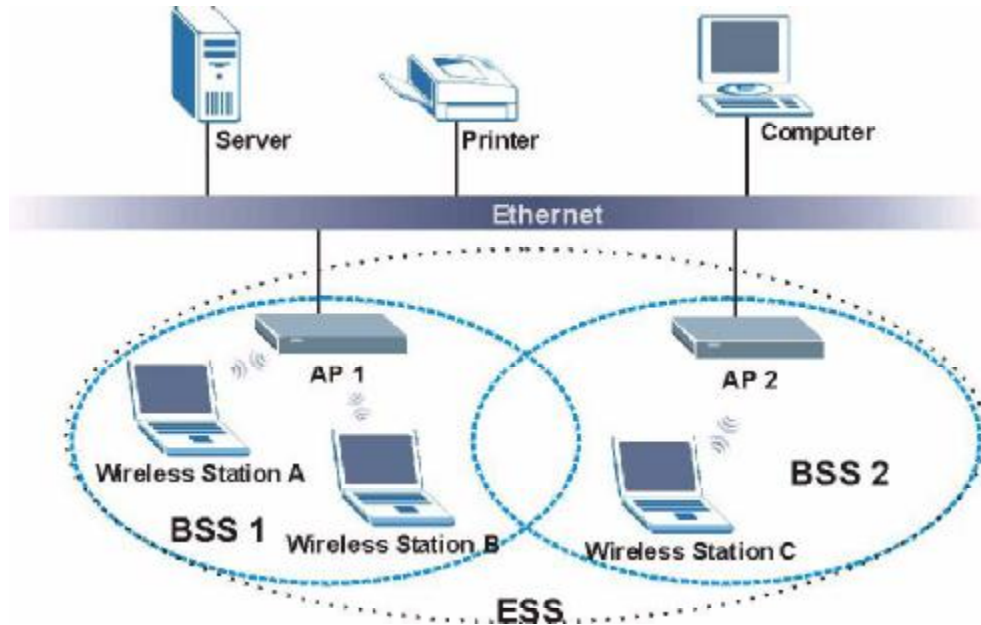
ESS

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 150 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.

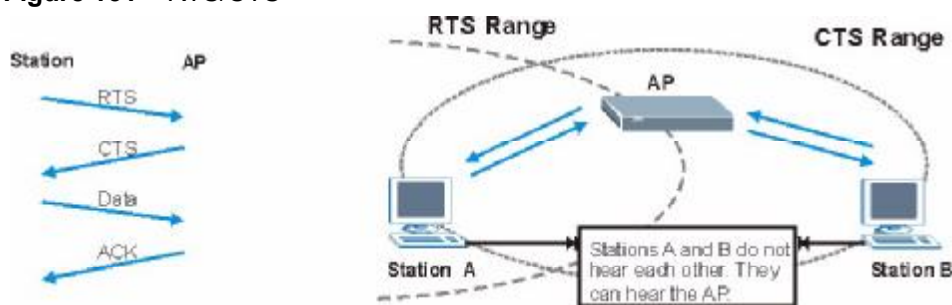
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel 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 151 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 78 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 79 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.

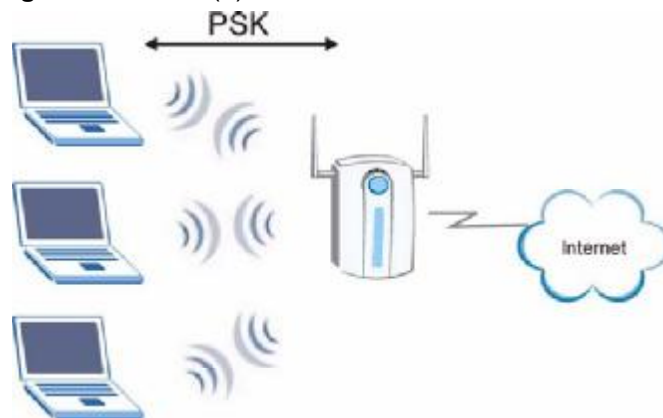
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

24.5.2 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 152 WPA(2)-PSK Authentication



24.5.3 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 80 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

F

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **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**.
 - 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 81 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
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	A popular videoconferencing solution from White Pines Software.
	TCP/UDP	24032	
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
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.

Table 81 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP	20	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
	TCP	21	
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 purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast 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.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP	137	The Network Basic Input/Output System is used for communication between computers in a LAN.
	TCP/UDP	138	
	TCP/UDP	139	
	TCP/UDP	445	
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.

Table 81 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
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.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
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	The Simple File Transfer Protocol is an old way of transferring files between computers.
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.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
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.

Table 81 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
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.
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 UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.



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.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

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.

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.

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.

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.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

A

Address Assignment [92](#)
 Alert [181](#)
 alternative subnet mask notation [220](#)
 AP [21](#)
 AP (Access Point) [247](#)
 AP Mode
 menu [56](#)
 overview [53](#)
 status screen [54](#)
 AP+Bridge [21](#)
 Auto-bridge [102](#)

B

Backup configuration [186](#)
 Bandwidth management
 application-based [147](#)
 overview [147](#)
 priority [153](#)
 services [154](#)
 subnet-based [147](#)
 BitTorrent [154](#)
 Bridge/Repeater [21](#)
 BSS [245](#)

C

CA [252](#)
 Certificate Authority [252](#)
 certifications [261](#)
 notices [263](#)
 viewing [264](#)
 Channel [31](#), [55](#), [247](#)
 Interference [247](#)
 channel [72](#)
 Configuration

 backup [186](#)
 reset the factory defaults [188](#)
 restore [187](#)
 content filtering [135](#)
 by keyword (in URL) [136](#)
 by web feature [136](#)
 copyright [261](#)
 CPU usage [31](#), [55](#)
 CTS (Clear to Send) [248](#)

D

Daylight saving [178](#)
 DDNS [123](#)
 see also Dynamic DNS
 service providers [124](#)
 DHCP [34](#), [107](#)
 DHCP server
 see also Dynamic Host Configuration Protocol
 DHCP client information [110](#)
 DHCP client list [110](#)
 DHCP server [104](#), [107](#)
 DHCP table [34](#), [110](#)
 DHCP client information
 DHCP status
 Dimensions [205](#)
 disclaimer [261](#)
 DNS [49](#), [109](#)
 DNS server
 see also Domain name system
 DNS Server [92](#)
 DNS server [109](#)
 Domain name [41](#)
 vs host name. see also system name
 Domain Name System [109](#)
 Domain Name System. See DNS.
 duplex setting [32](#), [56](#)
 Dynamic DNS [123](#)
 Dynamic Host Configuration Protocol [107](#)

Dynamic WEP Key Exchange [252](#)
DynDNS [124](#)
DynDNS see also DDNS [124](#)
DynDNS Wildcard [123](#)

E

EAP Authentication [251](#)
e-mail [86](#)
Encryption [253](#)
encryption [74](#)

- and local (user) database [74](#)
- key [75](#)
- WPA compatible [74](#)

ESS [246](#)
ESSID [200](#)
Extended Service Set [246](#)
Extended wireless security [43](#)

F

Factory LAN defaults [104](#), [107](#)
FCC interference statement [261](#)
File Transfer Program [154](#)
Firewall [130](#)

- Firewall overview guidelines [131](#)
- ICMP packets [132](#)
- network security
- Stateful inspection [130](#)
- ZyXEL device firewall [130](#)

firewall

- stateful inspection [129](#)

Firmware upload [183](#)

- file extension
- using HTTP

firmware version [31](#), [55](#)
Fragmentation Threshold [249](#)
FTP. see also File Transfer Program [154](#)

G

gateway [145](#)
General wireless LAN screen [75](#)

H

Hidden Node [247](#)
HTTP [154](#)
Hyper Text Transfer Protocol [154](#)

I

IANA [226](#)
IBSS [245](#)
IEEE 802.11g [249](#)
IGMP [93](#)

- see also Internet Group Multicast Protocol version

IGMP version [93](#)
Independent Basic Service Set [245](#)
Install UPnP [162](#)

- Windows Me [162](#)
- Windows XP [163](#)

Internet Assigned Numbers Authority

- See IANA

Internet connection

- Ethernet
- PPPoE. see also PPP over Ethernet
- PPTP
- WAN connection

Internet connection wizard [43](#)
Internet Group Multicast Protocol [93](#)
IP Address [105](#), [117](#)
IP address [48](#)

- dynamic

IP Pool [108](#)

L

LAN [103](#)

IP pool setup [104](#)
 LAN overview [103](#)
 LAN setup [103](#)
 LAN TCP/IP [104](#)
 Language [193](#)
 Link type [32, 55](#)
 local (user) database [73](#)
 and encryption [74](#)
 Local Area Network [103](#)
 Log [182](#)

M

MAC [80](#)
 MAC address [73, 93](#)
 cloning [51, 93](#)
 MAC address filter [73](#)
 MAC address filtering [80](#)
 MAC filter [80](#)
 managing the device
 good habits [22](#)
 using the web configurator. See web configurator.
 using the WPS. See WPS.
 MBSSID [21](#)
 Media access control [80](#)
 Memory usage [32, 55](#)
 Metric [146](#)
 mode [21](#)
 Multicast [93](#)
 IGMP [93](#)

N

NAT [113, 116, 225](#)
 global [114](#)
 how it works [115](#)
 inside [114](#)
 local [114](#)
 outside [114](#)
 overview [113](#)
 port forwarding [120](#)
 see also Network Address Translation

server [115](#)
 server sets [120](#)
 NAT traversal [159](#)
 Navigation Panel [32, 56](#)
 navigation panel [32, 56](#)
 NetBIOS [94](#)
 see also Network Basic Input/Output System [94](#)
 Network Address Translation [113, 116](#)

O

Operating Channel [31, 55](#)
 operating mode [21](#)

P

P2P [154](#)
 peer-to-peer [154](#)
 Point-to-Point Protocol over Ethernet [44, 96](#)
 Point-to-Point Tunneling Protocol [46, 98](#)
 Pool Size [108](#)
 Port forwarding [117, 120](#)
 default server [120](#)
 example [120](#)
 local server [117](#)
 port numbers
 services
 port speed [32, 56](#)
 Power Specification [205](#)
 PPPoE [44, 96](#)
 benefits [45](#)
 dial-up connection
 see also Point-to-Point Protocol over Ethernet [44](#)
 PPTP [46, 98](#)
 see also Point-to-Point Tunneling Protocol [46](#)
 Preamble Mode [249](#)
 product registration [264](#)

Q

Quality of Service (QoS) [83](#)

R

RADIUS [250](#)

 Shared Secret Key [251](#)

RADIUS Message Types [251](#)

RADIUS Messages [251](#)

RADIUS server [73](#)

registration

 product [264](#)

related documentation [3](#)

Remote management [155](#)

 and NAT [156](#)

 and the firewall [155](#)

 limitations [155](#)

 remote management session [155](#)

 system timeout [156](#)

Reset button [29](#), [188](#)

Reset the device [29](#)

Restore configuration [187](#)

RF (Radio Frequency) [206](#)

Roaming [82](#)

RTS (Request To Send) [248](#)

RTS Threshold [247](#), [248](#)

RTS/CTS Threshold [72](#), [82](#)

S

safety warnings [7](#)

Scheduling [88](#)

Security Parameters [256](#)

Service and port numbers [154](#)

Service Set [76](#)

Service Set IDentification [76](#)

Service Set IDentity. See SSID.

services

 and port numbers [257](#)

 and protocols [257](#)

Session Initiated Protocol [154](#)

SIP [154](#)

SSID [31](#), [55](#), [72](#), [76](#)

stateful inspection firewall [129](#)

Static DHCP [108](#)

Static Route [144](#)

Status [30](#)

subnet [217](#)

Subnet Mask [105](#)

subnet mask [49](#), [218](#)

subnetting [221](#)

Summary

 DHCP table [34](#)

 Packet statistics [35](#)

 Wireless station status [36](#)

syntax conventions [5](#)

Sys Op Mode [189](#)

System General Setup [175](#)

System Name [176](#)

System name [40](#)

 vs computer name

System restart [188](#)

T

TCP/IP configuration [107](#)

Temperature [205](#)

Time setting [177](#)

trademarks [261](#)

trigger port [121](#)

Trigger port forwarding [121](#)

 example [122](#)

 process [122](#)

U

Universal Plug and Play [159](#)

 application [160](#)

UPnP [159](#)

 forum [160](#)

 security issues [160](#)

URL Keyword Blocking [137](#)

Use Authentication [254](#)

user authentication [73](#)
 local (user) database [73](#)
 RADIUS server [73](#)

User Name [124](#)

V

VoIP [154](#)

VPN [98](#)

W

WAN

 IP address assignment [48](#)

WAN (Wide Area Network) [91](#)

WAN advanced [101](#)

WAN IP address [48](#)

WAN IP address assignment [50](#)

WAN MAC address [93](#)

warranty [264](#)

 note [264](#)

Web Configurator

 how to access [27](#)

 Overview [27](#)

Web configurator

 navigating [29](#)

web configurator [22](#)

WEP Encryption [78](#)

WEP encryption [77](#)

WEP key [77](#)

Wildcard [123](#)

Wireless association list [36](#)

wireless channel [200](#)

wireless LAN [200](#)

wireless LAN scheduling [88](#)

Wireless LAN wizard [42](#)

Wireless network

 basic guidelines [72](#)

 channel [72](#)

 encryption [74](#)

 example [71](#)

 MAC address filter [73](#)

 overview [71](#)

 security [72](#)

 SSID [72](#)

Wireless security [72](#)

 overview [72](#)

 type [72](#)

wireless security [200](#)

Wireless tutorial [53, 61](#)

 WPS [61](#)

Wizard setup [39](#)

 complete [52](#)

 Internet connection [43](#)

 system information [40](#)

 wireless LAN [42](#)

WLAN

 Interference [247](#)

 Security Parameters [256](#)

World Wide Web [154](#)

WPA compatible [74](#)

WPA, WPA2 [253](#)

WPS [22](#)

WWW [86, 154](#)

X

Xbox Live [154](#)

Z

ZyNOS [31, 55](#)

