

NBG4104

Wireless N-lite Managed Router

User's Guide



Default Login Details

| | |
|------------|--------------------|
| IP Address | http://192.168.1.1 |
| User Name | admin |
| Password | 1234 |

Firmware Version 1.0
Edition 1, 11/2011

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NBG4104 using the Web Configurator.

Tips for Reading User's Guides On-Screen

When reading a ZyXEL User's Guide On-Screen, keep the following in mind:

- If you don't already have the latest version of Adobe Reader, you can download it from <http://www.adobe.com>.
- Use the PDF's bookmarks to quickly navigate to the areas that interest you. Adobe Reader's bookmarks pane opens by default in all ZyXEL User's Guide PDFs.
- If you know the page number or know vaguely which page-range you want to view, you can enter a number in the toolbar in Reader, then press [ENTER] to jump directly to that page.
- Type [CTRL]+[F] to open the Adobe Reader search utility and enter a word or phrase. This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader.
- To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen.
- Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF.

Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get your NBG4104 up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

Refer to the included CD for support documents.

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.




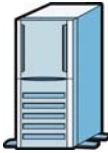

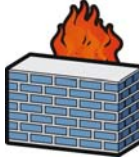




Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NBG4104 may be referred to as the "NBG4104", 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 NBG4104 icon is not an exact representation of your device.

| | | |
|--|---|---|
| NBG4104  | 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

| | |
|--|-----------|
| User's Guide | 15 |
| Introduction | 17 |
| The WPS Button | 20 |
| Introducing the Web Configurator | 21 |
| Monitor | 25 |
| NBG4104 Modes | 31 |
| Router Mode | 32 |
| Access Point Mode | 38 |
| Tutorials | 45 |
| Technical Reference | 53 |
| Wireless LAN | 55 |
| WAN | 69 |
| LAN | 81 |
| DHCP Server | 85 |
| NAT | 89 |
| DDNS | 95 |
| Static Route | 97 |
| VLAN Operation | 101 |
| Interface Group | 107 |
| Firewall | 111 |
| Content Filtering | 117 |
| Remote Management | 121 |
| Bandwidth Management | 130 |
| Universal Plug-and-Play (UPnP) | 136 |
| Maintenance | 143 |
| Troubleshooting | 151 |

Table of Contents

| | |
|--|-----------|
| About This User's Guide | 3 |
| Document Conventions | 4 |
| Safety Warnings..... | 6 |
| Contents Overview | 7 |
| Table of Contents | 9 |
| | |
| Part I: User's Guide | 15 |
| | |
| Chapter 1 | |
| Introduction..... | 17 |
| 1.1 Overview | 17 |
| 1.2 Applications | 17 |
| 1.3 Ways to Manage the NBG4104 | 17 |
| 1.4 Good Habits for Managing the NBG4104 | 17 |
| 1.5 LEDs | 18 |
| | |
| Chapter 2 | |
| The WPS Button..... | 20 |
| 2.1 Overview | 20 |
| | |
| Chapter 3 | |
| Introducing the Web Configurator | 21 |
| 3.1 Overview | 21 |
| 3.2 Accessing the Web Configurator | 21 |
| 3.2.1 Login Screen | 22 |
| 3.2.2 Password Screen | 22 |
| 3.3 Resetting the NBG4104 | 23 |
| 3.3.1 How to Use the RESET Button | 23 |
| | |
| Chapter 4 | |
| Monitor..... | 25 |
| 4.1 Overview | 25 |
| 4.2 What You Can Do | 25 |
| 4.3 The Log Screen | 25 |
| 4.3.1 View Log | 26 |

| | |
|---|-----------|
| 4.3.2 Log Settings | 26 |
| 4.4 DHCP Table | 26 |
| 4.5 Packet Statistics | 28 |
| 4.6 WLAN Station Status | 28 |
| Chapter 5 | |
| NBG4104 Modes | 31 |
| 5.1 Overview | 31 |
| 5.1.1 Device Modes | 31 |
| Chapter 6 | |
| Router Mode | 32 |
| 6.1 Overview | 32 |
| 6.2 Router Mode Status Screen | 33 |
| 6.2.1 Navigation Panel | 35 |
| Chapter 7 | |
| Access Point Mode | 38 |
| 7.1 Overview | 38 |
| 7.2 What You Can Do | 38 |
| 7.3 What You Need to Know | 38 |
| 7.3.1 Setting your NBG4104 to AP Mode | 39 |
| 7.3.2 Accessing the Web Configurator in Access Point Mode | 39 |
| 7.3.3 Configuring your WLAN and Maintenance Settings | 39 |
| 7.4 AP Mode Status Screen | 40 |
| 7.5 LAN Screen | 43 |
| Chapter 8 | |
| Tutorials | 45 |
| 8.1 Overview | 45 |
| 8.2 Set Up a Wireless Network with WPS | 45 |
| 8.2.1 Push Button Configuration (PBC) | 45 |
| 8.2.2 PIN Configuration | 46 |
| 8.3 Configure Wireless Security without WPS | 47 |
| 8.3.1 Configure Your Notebook | 49 |
| 8.4 Using Multiple SSIDs on the NBG4104 | 50 |
| 8.4.1 Configuring Security Settings of Multiple SSIDs | 51 |
| Part II: Technical Reference | 53 |
| Chapter 9 | |
| Wireless LAN | 55 |

| | |
|---|-----------|
| 9.1 Overview | 55 |
| 9.2 What You Can Do | 55 |
| 9.3 What You Should Know | 56 |
| 9.4 General Wireless LAN Screen | 58 |
| 9.5 Wireless Security | 60 |
| 9.5.1 No Security | 60 |
| 9.5.2 WEP Encryption | 60 |
| 9.5.3 WPA-PSK/WPA2-PSK | 62 |
| 9.6 MAC Filter | 62 |
| 9.7 Wireless LAN Advanced Screen | 63 |
| 9.8 Quality of Service (QoS) Screen | 65 |
| 9.9 WPS Screen | 65 |
| 9.10 WPS Station Screen | 66 |
| 9.11 Scheduling Screen | 67 |
| Chapter 10 | |
| WAN | 69 |
| 10.1 Overview | 69 |
| 10.2 What You Can Do | 69 |
| 10.3 What You Need To Know | 69 |
| 10.3.1 Configuring Your Internet Connection | 70 |
| 10.3.2 Multicast | 71 |
| 10.4 Management WAN | 72 |
| 10.4.1 Add/Edit Internet Connection | 73 |
| 10.4.2 Ethernet Encapsulation | 73 |
| 10.4.3 PPPoE Encapsulation | 75 |
| 10.4.4 Bridge Encapsulation | 78 |
| 10.5 Advanced WAN Screen | 79 |
| Chapter 11 | |
| LAN | 81 |
| 11.1 Overview | 81 |
| 11.2 What You Can Do | 81 |
| 11.3 What You Need To Know | 82 |
| 11.3.1 IP Pool Setup | 82 |
| 11.3.2 LAN TCP/IP | 82 |
| 11.3.3 IP Alias | 82 |
| 11.4 LAN IP Screen | 83 |
| 11.5 IP Alias Screen | 83 |
| Chapter 12 | |
| DHCP Server | 85 |
| 12.1 Overview | 85 |

| | |
|--|------------|
| 12.2 What You Can Do | 85 |
| 12.3 What You Need To Know | 85 |
| 12.4 The DHCP General Screen | 86 |
| 12.5 The DHCP Advanced Screen | 87 |
| Chapter 13 | |
| NAT..... | 89 |
| 13.1 Overview | 89 |
| 13.2 What You Can Do | 90 |
| 13.3 What You Need To Know | 90 |
| 13.4 The NAT General Screen | 92 |
| 13.5 The NAT Application Screen | 92 |
| Chapter 14 | |
| DDNS..... | 95 |
| 14.1 Overview | 95 |
| 14.2 What You Need To Know | 95 |
| 14.3 The DDNS General Screen | 96 |
| Chapter 15 | |
| Static Route..... | 97 |
| 15.1 Overview | 97 |
| 15.2 IP Static Route Screen | 98 |
| Chapter 16 | |
| VLAN Operation..... | 101 |
| 16.1 Overview | 101 |
| 16.2 What You Can Do | 101 |
| 16.3 LAN To WAN Screen | 101 |
| 16.3.1 Add/Edit VLAN Rule | 103 |
| 16.4 WAN To LAN Screen | 105 |
| Chapter 17 | |
| Interface Group..... | 107 |
| 17.1 Overview | 107 |
| 17.2 The Interface Group Screen | 107 |
| 17.2.1 Interface Group Configuration | 108 |
| Chapter 18 | |
| Firewall..... | 111 |
| 18.1 Overview | 111 |
| 18.2 What You Can Do | 111 |
| 18.3 What You Need To Know | 112 |

| | |
|--|------------|
| 18.4 The Firewall General Screen | 113 |
| 18.5 The Access Control Rule Screen | 114 |
| 18.5.1 Access Control Rule Edit | 115 |
| 18.6 The Services Screen | 116 |
| Chapter 19 | |
| Content Filtering..... | 117 |
| 19.1 Overview | 117 |
| 19.2 What You Need To Know | 117 |
| 19.3 Content Filter | 118 |
| 19.4 Technical Reference | 119 |
| 19.4.1 Customizing Keyword Blocking URL Checking | 119 |
| Chapter 20 | |
| Remote Management..... | 121 |
| 20.1 Overview | 121 |
| 20.2 What You Need to Know | 121 |
| 20.2.1 Remote Management and NAT | 121 |
| 20.3 What You Can Do | 121 |
| 20.4 The WWW Screen | 122 |
| 20.5 The Telnet Screen | 123 |
| 20.6 The FTP Screen | 124 |
| 20.7 The SNMP Screen | 124 |
| 20.8 The TR069 Screen | 127 |
| 20.9 The Import CA Screen | 128 |
| Chapter 21 | |
| Bandwidth Management..... | 130 |
| 21.1 Overview | 130 |
| 21.2 What You Can Do | 130 |
| 21.3 What You Need To Know | 130 |
| 21.4 The Bandwidth MGMT General Screen | 131 |
| 21.5 The Bandwidth MGMT Advanced Screen | 132 |
| 21.5.1 User Defined Service Rule Configuration | 134 |
| 21.5.2 Services and Port Numbers | 135 |
| Chapter 22 | |
| Universal Plug-and-Play (UPnP)..... | 136 |
| 22.1 Overview | 136 |
| 22.2 What You Need to Know | 136 |
| 22.2.1 NAT Traversal | 136 |
| 22.2.2 Cautions with UPnP | 136 |
| 22.3 UPnP Screen | 137 |

| | |
|--|------------|
| 22.4 Technical Reference | 137 |
| 22.4.1 Using UPnP in Windows XP Example | 137 |
| 22.4.2 Web Configurator Easy Access | 140 |
| Chapter 23 | |
| Maintenance | 143 |
| 23.1 Overview | 143 |
| 23.2 What You Can Do | 143 |
| 23.3 General Screen | 143 |
| 23.4 Password Screen | 144 |
| 23.5 Time Setting Screen | 145 |
| 23.6 Firmware Upgrade Screen | 146 |
| 23.7 Configuration Backup/Restore Screen | 147 |
| 23.8 Restart Screen | 148 |
| 23.9 System Operation Mode | 149 |
| 23.10 Sys OP Mode Screen | 150 |
| Chapter 24 | |
| Troubleshooting..... | 151 |
| 24.1 Overview | 151 |
| 24.2 Power, Hardware Connections, and LEDs | 151 |
| 24.3 NBG4104 Access and Login | 152 |
| 24.4 Internet Access | 154 |
| 24.5 Resetting the NBG4104 to Its Factory Defaults | 155 |
| 24.6 Wireless Router/AP Troubleshooting | 155 |
| Appendix A Product Specifications | 159 |
| 24.7 Wall-mounting Instructions | 161 |
| Appendix B Pop-up Windows, JavaScript and Java Permissions | 163 |
| Appendix C IP Addresses and Subnetting..... | 175 |
| Appendix D Setting Up Your Computer's IP Address | 185 |
| Appendix E Wireless LANs..... | 213 |
| Appendix F Common Services | 227 |
| Appendix G Legal Information | 231 |
| Index | 241 |

PART I

User's Guide

Introduction

1.1 Overview

This chapter introduces the main features and applications of the NBG4104.

The NBG4104 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.

1.2 Applications

You can create the following networks using the NBG4104:

- **Wired.** You can connect network devices via the Ethernet ports of the NBG4104 so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the NBG4104 to access network resources.
- **WAN.** Connect to a broadband modem/router for Internet access.
- **WPS.** Create an instant network connection with another WPS-compatible device, sharing your network connection with it.

1.3 Ways to Manage the NBG4104

Use any of the following methods to manage the NBG4104.

- **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 NBG4104 using a (supported) web browser.

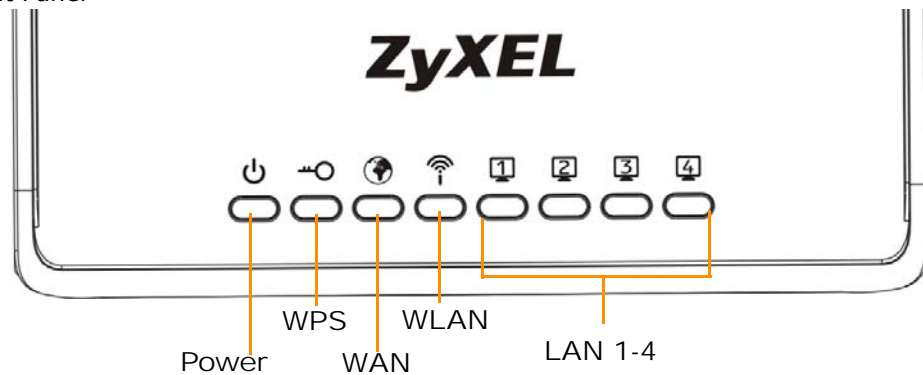
1.4 Good Habits for Managing the NBG4104

Do the following things regularly to make the NBG4104 more secure and to manage the NBG4104 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 NBG4104 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG4104. You could simply restore your last configuration.

1.5 LEDs

Figure 1 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 NBG4104 is receiving power and functioning properly. |
| | | Blinking | The NBG4104 is booting up. |
| | Off | The NBG4104 is not receiving power. | |
| WPS | Green | On | The WPS status is configured. |
| | | Blinking | The NBG4104 is negotiating a WPS connection with a wireless client. |
| | Off | The WPS function is disabled on the NBG4104. | |
| WAN | Green | On | The NBG4104's WAN connection is ready. |
| | | Blinking | The NBG4104 is sending/receiving data through the WAN with a 10/100Mbps transmission rate. |
| | Off | The WAN connection is not ready, or has failed. | |
| WLAN | Green | On | The NBG4104 is ready, but is not sending/receiving data through the wireless LAN. |
| | | Blinking | The NBG4104 is sending/receiving data through the wireless LAN. |
| | Off | The wireless LAN is not ready or has failed. | |

Table 1 Front panel LEDs and WPS button (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|---------|-------|---|--|
| LAN 1-4 | Green | On | The NBG4104's LAN connection is ready. |
| | | Blinking | The NBG4104 is sending/receiving data through the LAN with a 10/100Mbps transmission rate. |
| | Off | The LAN connection is not ready, or has failed. | |

The WPS Button

2.1 Overview

Your NBG4104 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 8.2 on page 45](#).

Introducing the Web Configurator

3.1 Overview

This chapter describes how to access the NBG4104 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the NBG4104 via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

Refer to the Troubleshooting chapter ([Chapter 24 on page 151](#)) to see how to make sure these functions are allowed in Internet Explorer.

3.2 Accessing the Web Configurator

- 1 Make sure your NBG4104 hardware is properly connected and prepare your computer or computer network to connect to the NBG4104 (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "http://192.168.1.1" as the website address.

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

3.2.1 Login Screen

The Web Configurator initially displays the following login screen.

Figure 2 Login screen



The following table describes the labels in this screen.

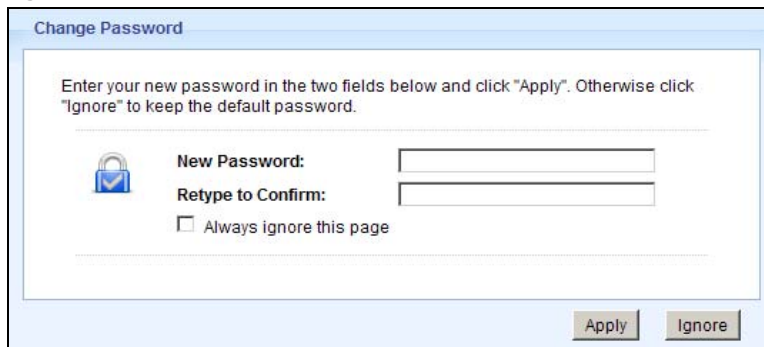
Table 2 Login screen

| LABEL | DESCRIPTION |
|-----------|---|
| User Name | Type "admin" (default) as the user name. |
| Password | Type "1234" (default) as the password. |
| Login | Click Login to enter the NBG4104's web configurator. |

3.2.2 Password Screen

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

Figure 3 Change Password Screen



The following table describes the labels in this screen.

Table 3 Change Password Screen

| LABEL | DESCRIPTION |
|-------------------|--|
| New Password | Type a new password. |
| Retype to Confirm | Retype the password for confirmation. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Ignore | Click Ignore if you do not want to change the password this time. |

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to [Chapter 23 on page 143](#) to change this). Simply log back into the NBG4104 if this happens.

3.3 Resetting the NBG4104

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 NBG4104 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 How to Use the RESET Button

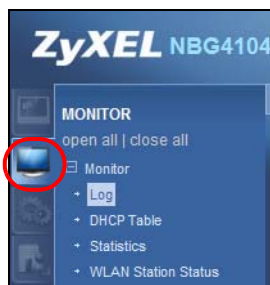
- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the NBG4104.
- 3 Press the **RESET** button for longer than 5 seconds to set the NBG4104 back to its factory-default configurations.

Monitor

4.1 Overview

This chapter discusses read-only information related to the device state of the NBG4104.

To access the Monitor screens, click . Click **open all** to show the complete menu.



You can also click the links in the **Summary** table of the **Status** screen to view the bandwidth consumed, packets sent/received as well as the status of clients connected to the NBG4104.

4.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the NBG4104 ([Section 4.3 on page 25](#)).
- Use the **DHCP Table** screen to view information related to your DHCP status ([Section 4.4 on page 26](#)).
- use the **Statistics** screen to view port statistics and the "system up time" ([Section 4.5 on page 28](#)).
- Use the **WLAN Station Status** screen to view the wireless stations that are currently associated to the NBG4104 ([Section 4.6 on page 28](#)).

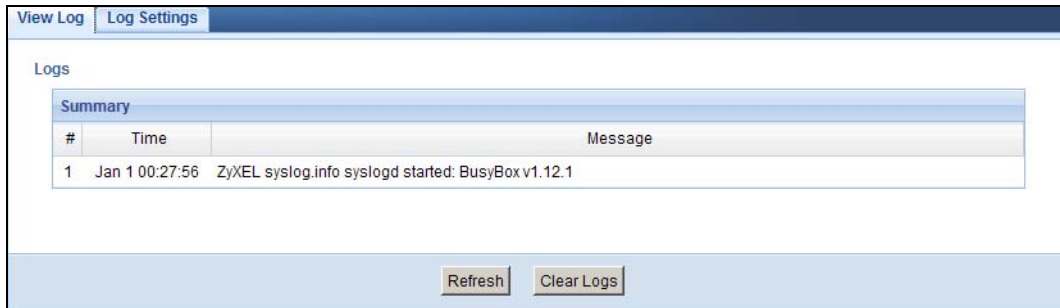
4.3 The Log Screen

The Web Configurator allows you to look at all of the NBG4104's logs in one location.

4.3.1 View Log

Click **Monitor > Log** to open the **View Log** screen. You can see the logged messages for the NBG4104. The log wraps around and deletes the old entries after it fills. Click **Clear Logs** to delete all the logs. Click **Refresh** to renew the log screen.

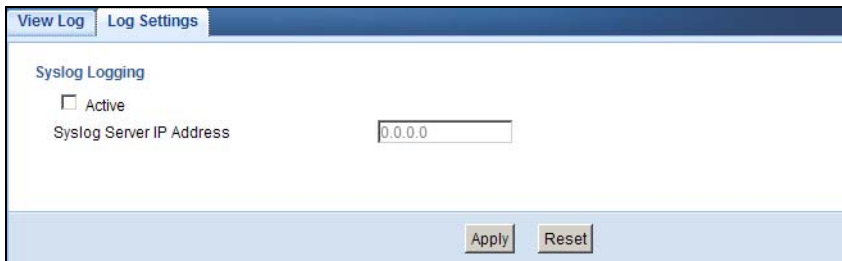
Figure 4 View Log



4.3.2 Log Settings

Click **Monitor > Log** to open the **Log Settings** screen. You can configure syslog settings.

Figure 5 Log Settings



The following table describes the labels in this screen.

Table 4 Monitor > Log > Log Settings

| LABEL | DESCRIPTION |
|--------------------------|---|
| Active | Select this to enable syslog logging. |
| Syslog Server IP Address | Enter the server name or IP address of the syslog server that logs the selected categories of logs. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

4.4 DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG4104's LAN as a DHCP server or disable it. When configured as a server, the NBG4104 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 or **Monitor > DHCP Table**. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **Host Name**, **IP Address**, and **Mac Address**) of all network clients using the NBG4104's DHCP server.

Figure 6 Summary: DHCP Table

The screenshot shows a web interface titled "DHCP Table". Inside, there is a section labeled "DHCP Client Table" containing a table with the following data:

| # | IP Address | Host Name | MAC Address |
|---|-------------|--------------|-------------------|
| 1 | 192.168.1.2 | twpc13774-02 | 00:24:21:7E:20:96 |

Below the table is a "Refresh" button.

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. |

4.5 Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen or **Monitor > Statistics**. Read-only information here includes port 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

The screenshot shows a web interface for 'Statistics'. It features a table with the following data:

| Port | TxPkts | RxPkts | TxBytes | RxBytes |
|--------|--------|--------|---------|---------|
| WAN | 7 | 0 | 4158 | 0 |
| LAN | 693 | 779 | 450417 | 75369 |
| WLAN | 0 | 0 | 0 | 0 |
| WLAN 2 | 0 | 0 | 0 | 0 |
| WLAN 3 | 0 | 0 | 0 | 0 |
| WLAN 4 | 0 | 0 | 0 | 0 |

Below the table, it displays 'System Up Time: 0 day: 0 hour: 1 minute'. At the bottom, there is a 'Poll interval(s):' field with the value '10' and three buttons: 'Set Interval', 'Stop', and 'Refresh'.

The following table describes the labels in this screen.

Table 6 Summary: Packet Statistics

| LABEL | DESCRIPTION |
|------------------|--|
| Port | This is the NBG4104's port type. |
| TxPkts | This is the number of transmitted packets on this port. |
| RxPkts | This is the number of received packets on this port. |
| TxBytes | This displays the transmission speed in bytes per second on this port. |
| RxBytes | This displays the reception speed in bytes per second on this port. |
| Up Time | This is the total time the NBG4104 has been for each session. |
| System Up Time | This is the total time the NBG4104 has been on. |
| Poll Interval(s) | Enter the time interval in seconds for refreshing statistics in this field. |
| Set Interval | Click this button to apply the new poll interval you entered in the Poll Interval(s) field. |
| Stop | Click Stop to stop refreshing statistics. |
| Refresh | Click Refresh to renew the screen. |

4.6 WLAN Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen or **Monitor > WLAN Station Status**. View the wireless stations that are currently associated to the NBG4104 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 |
|---|-------------------|---------------------|
| 1 | 00:22:FB:65:9A:F4 | 03:39:07 1970/01/01 |

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 NBG4104's WLAN network. |
| Refresh | Click Refresh to reload the list. |

NBG4104 Modes

5.1 Overview

This chapter introduces the operating mode of your NBG4104, or simply how the NBG4104 is being used in the network.

5.1.1 Device Modes

These are the operating mode of the NBG4104:

- **Router:** This is the default device mode of the NBG4104. Use this mode to connect the local network to another network, like the Internet. Go to [Section 6.2 on page 33](#) to view the **Status** screen in this mode.
- **Access Point:** Use this mode if you want to extend your network by allowing network devices to connect to the NBG4104 wirelessly. Go to [Section 7.4 on page 40](#) to view the **Status** screen in this mode.

For more information on these modes and to change the mode of your NBG4104, refer to [Chapter 23 on page 150](#).

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

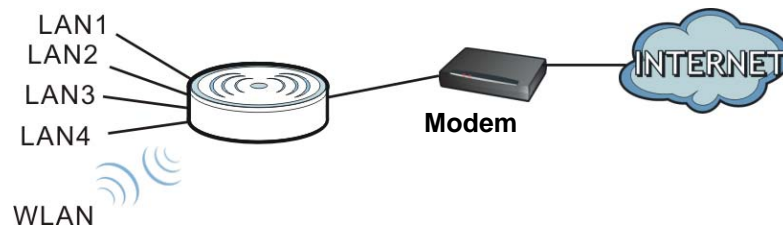
When changing to another mode, the IP address of the NBG4104 changes. The running applications and services of the network devices connected to the NBG4104 can be interrupted.

Router Mode

6.1 Overview

The NBG4104 is set to router mode by default. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the NBG4104 connects the local network (**LAN1 ~ LAN4**) to the Internet.

Figure 9 NBG4104 Network



6.2 Router Mode Status Screen


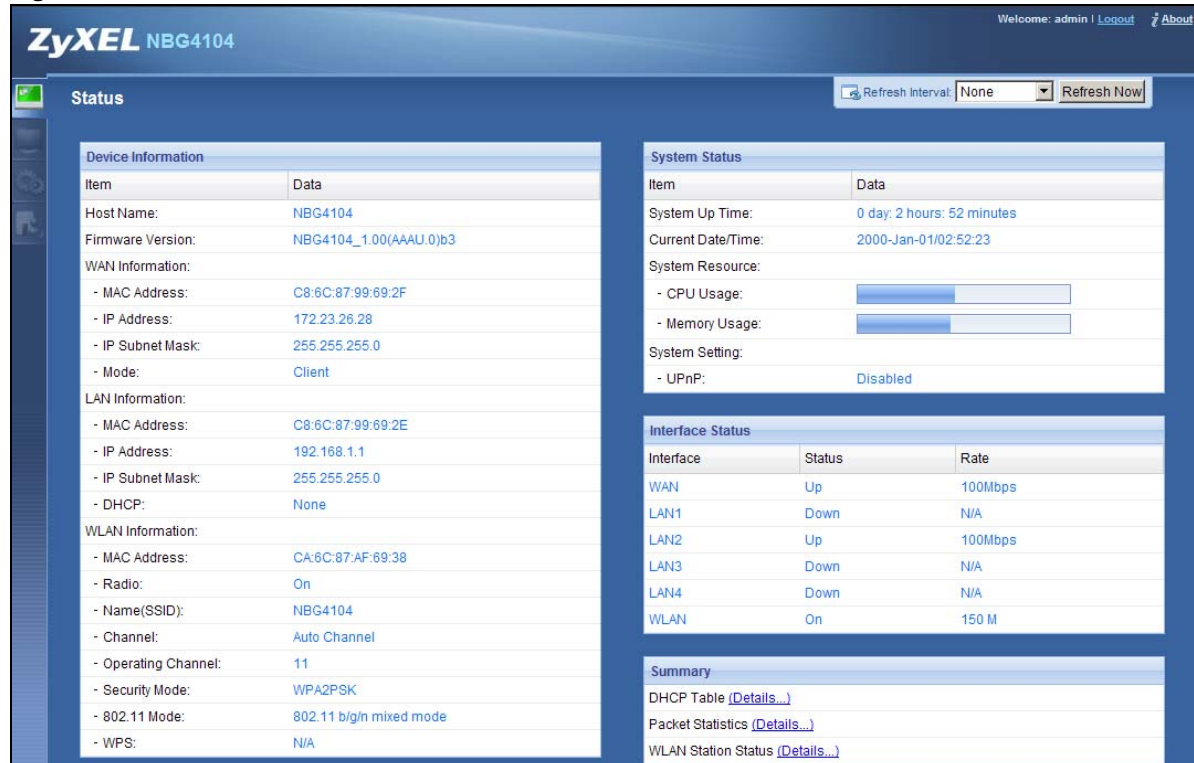



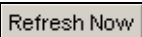




Click  to open the status screen.

Figure 10 Status Screen: Router Mode



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

Table 8 Status Screen Icon Key: Router Mode

| ICON | DESCRIPTION |
|---|---|
|  | Click this at any time to exit the Web Configurator. |
|  | Click this icon to view copyright and a link for related product information. |
|  | 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. |
|  | Click this icon to see the Status page. The information in this screen depends on the device mode you select. |
|  | Click this icon to see the Monitor navigation menu. |
|  | Click this icon to see the Configuration navigation menu. |
|  | Click this icon to see the Maintenance navigation menu. |

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

Table 9 Status Screen: Router Mode

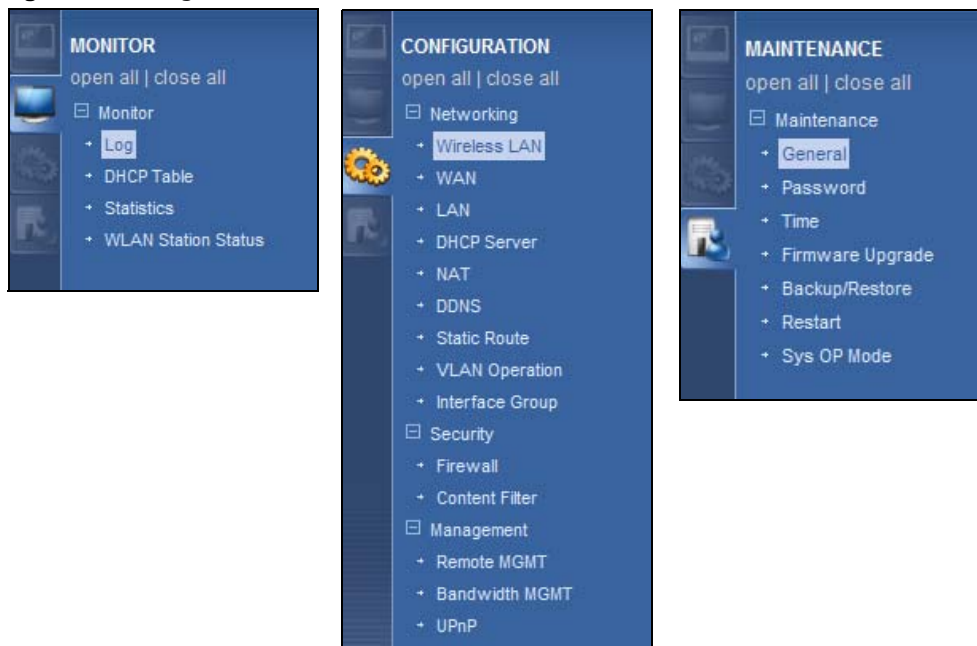
| LABEL | DESCRIPTION |
|---------------------|---|
| Device Information | |
| Host Name | This is the device's host name. |
| Firmware Version | This is the firmware version. |
| WAN Information | |
| - MAC Address | This shows the WAN Ethernet adapter MAC Address of your device. |
| - IP Address | This shows the WAN port's IP address. |
| - IP Subnet Mask | This shows the WAN port's subnet mask. |
| - Mode | This shows the device mode to which the NBG4104 is set. |
| 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 Disable . |
| WLAN Information | |
| - MAC Address | This shows the wireless adapter MAC Address of your device. |
| - Radio | This shows the current status of the Wireless LAN - ON or OFF . |
| - Name (SSID) | This shows a descriptive name used to identify the NBG4104 in the wireless LAN. |
| - Channel | This shows the channel number which you select manually. |
| - Operating Channel | This shows the channel number which the NBG4104 is currently using over the wireless LAN. |
| - Security Mode | This shows the level of wireless security the NBG4104 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 | |
| Item | This column shows the type of data the NBG4104 is recording. |
| Data | This column shows the actual data recorded by the NBG4104. |
| System Up Time | This is the total time the NBG4104 has been on. |
| Current Date/Time | This field displays your NBG4104's present date and time. |
| System Resource | |
| - CPU Usage | This displays what percentage of the NBG4104's processing ability is currently used. When this percentage is close to 100%, the NBG4104 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 NBG4104 is using. |
| System Setting | |
| - UPnP | This shows whether UPnP is enabled or not. |
| Interface Status | |
| Interface | This displays the NBG4104 port types. The port types are: WAN , LAN and WLAN . |

Table 9 Status Screen: Router Mode (continued)

| LABEL | DESCRIPTION |
|---------------------|--|
| Status | For the LAN and WAN ports, this field displays Down (line is down) or Up (line is up or connected). For the WLAN, it displays Up when the WLAN is enabled or Down when the WLAN is disabled. |
| Rate | For the LAN ports, this displays the port speed and duplex setting or N/A when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation. 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 | Click Details... to go to the Monitor > DHCP Table screen (Section 4.4 on page 26). Use this screen to view current DHCP client information. |
| Packet Statistics | Click Details... to go to the Monitor > Packet Statistics screen (Section 4.5 on page 28). Use this screen to view port status and packet specific statistics. |
| WLAN Station Status | Click Details... to go to the Monitor > WLAN Station Status screen (Section 4.6 on page 28). Use this screen to view the wireless stations that are currently associated to the NBG4104. |

6.2.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG4104 features.

Figure 11 Navigation Panel: Router Mode

The following table describes the sub-menus.

Table 10 Navigation Panel: Router Mode

| LINK | TAB | FUNCTION |
|----------------------|-----------------|---|
| Status | | This screen shows the NBG4104's general device, system and interface status information. Use this screen to access the summary statistics tables. |
| MONITOR | | |
| Log | | Use this screen to view the list of activities recorded by your NBG4104. |
| DHCP Table | | Use this screen to view current DHCP client information. |
| 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 NBG4104. |
| CONFIGURATION | | |
| Networking | | |
| Wireless LAN | General | Use this screen to configure wireless LAN and the level of wireless security for the NBG4104. |
| | MAC Filter | Use the MAC filter screen to configure the NBG4104 to block access to devices or block the devices from accessing the NBG4104. |
| | Advanced | This screen allows you to configure advanced wireless settings. |
| | QoS | Use this screen to enable 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 | Management WAN | This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers, the WAN MAC address, and VLAN settings. |
| | Advanced | Use this screen to configure multicast and auto-subnet. |
| LAN | IP | Use this screen to configure LAN IP address and subnet mask. |
| | IP Alias | Use this screen to have the NBG4104 apply IP alias to create LAN subnets. |
| DHCP Server | General | Use this screen to enable the NBG4104's DHCP server. |
| | Advanced | Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server. |
| NAT | General | Use this screen to enable NAT. |
| | Application | Use this screen to configure servers behind the NBG4104. |
| DDNS | General | Use this screen to set up dynamic DNS. |
| Static Route | IP Static Route | Use this screen to configure IP static routes. |
| VLAN Operation | LAN to WAN | Use this screen to configure QoS rules and actions for LAN to WAN traffic. |
| | WAN to LAN | Use this screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent out through individual LAN ports. |
| Interface Group | Interface Group | Use this screen to add a LAN interface or a VLAN ID to a new group. |
| Security | | |

Table 10 Navigation Panel: Router Mode (continued)

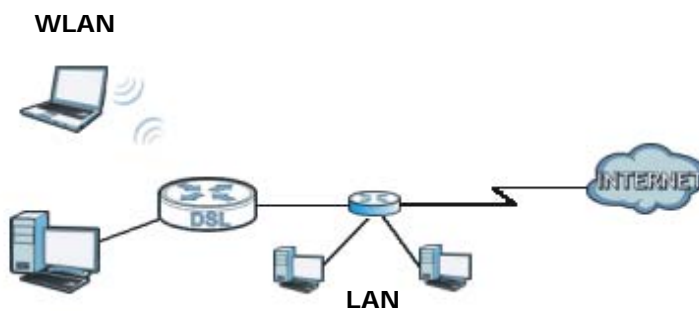
| LINK | TAB | FUNCTION |
|--------------------|---------------------|--|
| Firewall | General | Use this screen to activate/deactivate the firewall and Anti-Dos Attack. |
| | Access Control Rule | This screen shows a summary of the firewall rules, and allows you to edit/delete a firewall rule. |
| | Services | Use this screen to configure ICMP setting of the NBG4104. |
| Content Filter | Content Filter | Use this screen to block sites containing certain keywords in the URL. |
| Management | | |
| Remote MGMT | WWW | Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP or HTTPs to manage the NBG4104. |
| | TELNET | Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG4104. |
| | FTP | Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to manage the NBG4104. |
| | SNMP | Use this screen to configure through which interface(s) and from which IP address(es) users can use SNMP to manage the NBG4104. |
| | TR069 | Use this screen to configure the NBG4104's TR-069 auto-configuration settings. |
| | Import CA | Use this screen to import CA certificates to the NBG4104. |
| Bandwidth MGMT | General | Use this screen to configure a bandwidth management service type. |
| | Advanced | Use this screen to configure bandwidth management for specific types of applications. |
| UPnP | General | Use this screen to enable UPnP on the NBG4104. |
| MAINTENANCE | | |
| General | General | Use this screen to view and change administrative settings such as system and domain names. |
| Password | Password Setup | Use this screen to change the password of your NBG4104. |
| Time | Time Setting | Use this screen to change your NBG4104's time and date. |
| Firmware Upgrade | Firmware Upgrade | Use this screen to upload firmware to your NBG4104. |
| Backup/Restore | Backup/Restore | Use this screen to backup and restore the configuration or reset the factory defaults to your NBG4104. |
| Reset/Restart | Restart | This screen allows you to reboot the NBG4104 without turning the power off. |
| Sys OP Mode | Sys OP Mode | This screen allows you to select whether your device acts as a Router or a Access Point. |

Access Point Mode

7.1 Overview

Use your NBG4104 as an access point (AP) if you already have a router or gateway on your network. In this mode your NBG4104 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 12 Wireless Internet Access in Access Point Mode



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

Note: See [Chapter 8 on page 45](#) for an example of setting up a wireless network in Access Point mode.

7.2 What You Can Do

- Use the **Status** screen to view read-only information about your NBG4104 ([Section 7.4 on page 40](#)).
- Use the **LAN** screen to set the IP address for your NBG4104 acting as an access point ([Section 7.5 on page 43](#)).

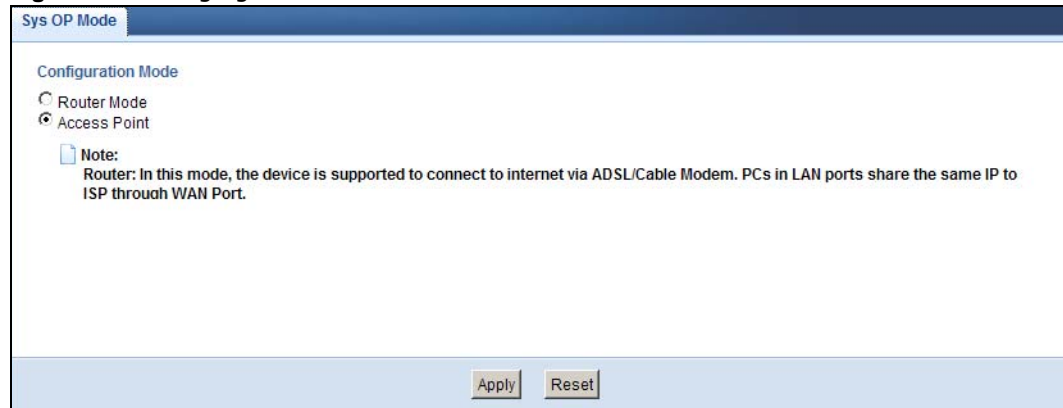
7.3 What You Need to Know

See [Chapter 8 on page 45](#) for a tutorial on setting up a network with the NBG4104 as an access point.

7.3.1 Setting your NBG4104 to AP Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To use your NBG4104 as an access point, go to **Maintenance > Sys OP Mode > General** and select **Access Point mode**.

Figure 13 Changing to Access Point mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG4104 is already in Access Point mode.

7.3.2 Accessing the Web Configurator in Access Point Mode

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

- 1 Connect your computer to the LAN port of the NBG4104.
- 2 The default IP address of the NBG4104 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix D on page 185](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

7.3.3 Configuring your WLAN and Maintenance Settings

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

- See [Chapter 9 on page 55](#) for information on the configuring your wireless network.
- See [Chapter 23 on page 143](#) for information on configuring your **Maintenance** settings.

7.4 AP Mode Status Screen


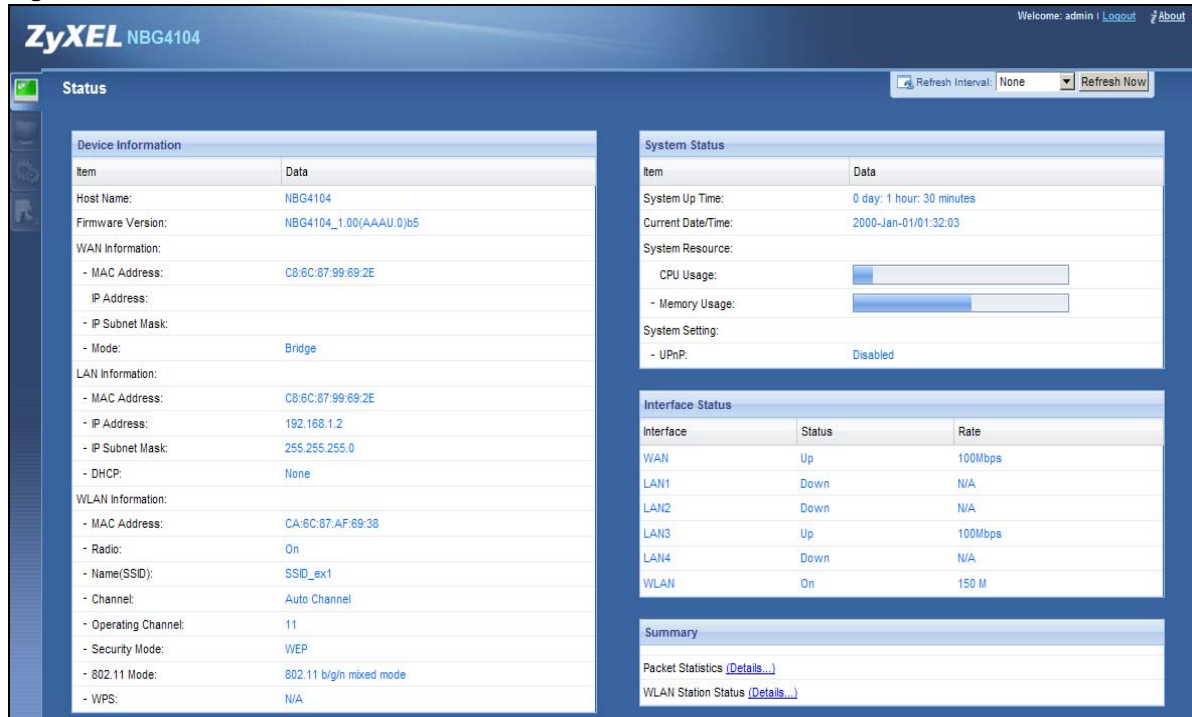
Click  to open the **Status** screen.

Figure 14 Status Screen: Access Point Mode



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

Table 11 Status Screen: AP Mode

| LABEL | DESCRIPTION |
|--------------------|---|
| Device Information | |
| Host Name | This is the device's host name. |
| Firmware Version | This is the firmware version. |
| 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. |
| - Mode | This shows the device mode to which the NBG4104 is set. |
| 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. In AP mode, this field shows None , meaning DHCP is disabled. |
| WLAN Information | |
| - MAC Address | This shows the wireless adapter MAC Address of your device. |
| - Radio | This shows the current status of the Wireless LAN - ON or OFF . |

Table 11 Status Screen: AP Mode (continued)

| LABEL | DESCRIPTION |
|---------------------|--|
| - Name (SSID) | This shows a descriptive name used to identify the NBG4104 in the wireless LAN. |
| - Channel | This shows the channel number which you select manually. |
| - Operating Channel | This shows the channel number which the NBG4104 is currently using over the wireless LAN. |
| - Security Mode | This shows the level of wireless security the NBG4104 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 | |
| Item | This column shows the type of data the NBG4104 is recording. |
| Data | This column shows the actual data recorded by the NBG4104. |
| System Up Time | This is the total time the NBG4104 has been on. |
| Current Date/Time | This field displays your NBG4104's present date and time. |
| System Resource | |
| - CPU Usage | This displays what percentage of the NBG4104's processing ability is currently used. When this percentage is close to 100%, the NBG4104 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 NBG4104 is using. |
| System Setting | |
| - UPnP | This shows whether UPnP is enabled or not. |
| Interface Status | |
| Interface | This displays the NBG4104 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. 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 | |
| Packet Statistics | Click Details... to go to the Monitor > Packet Statistics screen (Section 4.5 on page 28). Use this screen to view port status and packet specific statistics. |
| WLAN Station Status | Click Details... to go to the Monitor > WLAN Station Status screen (Section 4.6 on page 28). Use this screen to view the wireless stations that are currently associated to the NBG4104. |

7.4.0.1 Navigation Panel

Use the menu in the navigation panel to configure NBG4104 features in **Access Point** mode.

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

Figure 15 Menu: Access Point Mode



The following table describes the sub-menus.

Table 12 Navigation Panel: AP Mode

| LINK | TAB | FUNCTION |
|----------------------|-------------|---|
| Status | | This screen shows the NBG4104's general device, system and interface status information. Use this screen to access the summary statistics tables. |
| MONITOR | | |
| Log | | Use this screen to view the list of activities recorded by your NBG4104. |
| 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 NBG4104. |
| CONFIGURATION | | |
| Networking | | |
| Wireless LAN | General | Use this screen to configure wireless LAN and the level of wireless security for the NBG4104. |
| | MAC Filter | Use the MAC filter screen to configure the NBG4104 to block access to devices or block the devices from accessing the NBG4104. |
| | Advanced | This screen allows you to configure advanced wireless settings. |
| | QoS | Use this screen to enable 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. |
| | IP Alias | Use this screen to have the NBG4104 apply IP alias to create LAN subnets. |
| VLAN Operation | LAN to WAN | Use this screen to configure QoS rules and actions for LAN to WAN traffic. |
| | WAN to LAN | Use this screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent out through individual LAN ports. |

Table 12 Navigation Panel: AP Mode (continued)

| LINK | TAB | FUNCTION |
|--------------------|------------------|--|
| Interface Group | Interface Group | Use this screen to add a LAN interface or a VLAN ID to a new group. |
| Management | | |
| Remote MGMT | WWW | Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP or HTTPs to manage the NBG4104. |
| | TELNET | Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG4104. |
| | FTP | Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to manage the NBG4104. |
| | SNMP | Use this screen to configure through which interface(s) and from which IP address(es) users can use SNMP to manage the NBG4104. |
| | TR069 | Use this screen to configure the NBG4104's TR-069 auto-configuration settings. |
| | Import CA | Use this screen to import CA certificates to the NBG4104. |
| MAINTENANCE | | |
| General | General | Use this screen to view and change administrative settings such as system and domain names. |
| Password | Password Setup | Use this screen to change the password of your NBG4104. |
| Time | Time Setting | Use this screen to change your NBG4104's time and date. |
| Firmware Upgrade | Firmware Upgrade | Use this screen to upload firmware to your NBG4104. |
| Backup/Restore | Backup/Restore | Use this screen to backup and restore the configuration or reset the factory defaults to your NBG4104. |
| Reset/Restart | Restart | This screen allows you to reboot the NBG4104 without turning the power off. |
| Sys OP Mode | Sys OP Mode | This screen allows you to select whether your device acts as a Router or a Access Point. |

7.5 LAN Screen

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

Click **Configuration > Networking > LAN** to see the screen below.

Note: If you change the IP address of the NBG4104 in the screen below, you will need to log into the NBG4104 again using the new IP address.

Figure 16 Configuration > Networking > LAN > IP

The screenshot shows the 'IP' configuration screen for the LAN TCP/IP settings. The 'IP Address' field is set to 192.168.1.2 and the 'IP Subnet Mask' field is set to 255.255.255.0. There are 'Apply' and 'Reset' buttons at the bottom of the screen.

The table below describes the labels in the screen.

Table 13 Configuration > Networking > 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 NBG4104 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 NBG4104. |
| Apply | Click Apply to save your changes to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |

8.1 Overview

This chapter provides tutorials for setting up your NBG4104.

- [Set Up a Wireless Network with WPS](#)
- [Configure Wireless Security without WPS](#)
- [Using Multiple SSIDs on the NBG4104](#)

8.2 Set Up a Wireless Network with WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG4104 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 8.2.1 on page 45](#). 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 NBG4104's interface. See [Section 8.2.2 on page 46](#). This is the more secure method, since one device can authenticate the other.

8.2.1 Push Button Configuration (PBC)

- 1 Make sure that your NBG4104 is turned on. Make sure the device is placed 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 NBG4104's Web Configurator and press the **Push Button** in the **Configuration > Networking > Wireless LAN > WPS Station** screen.

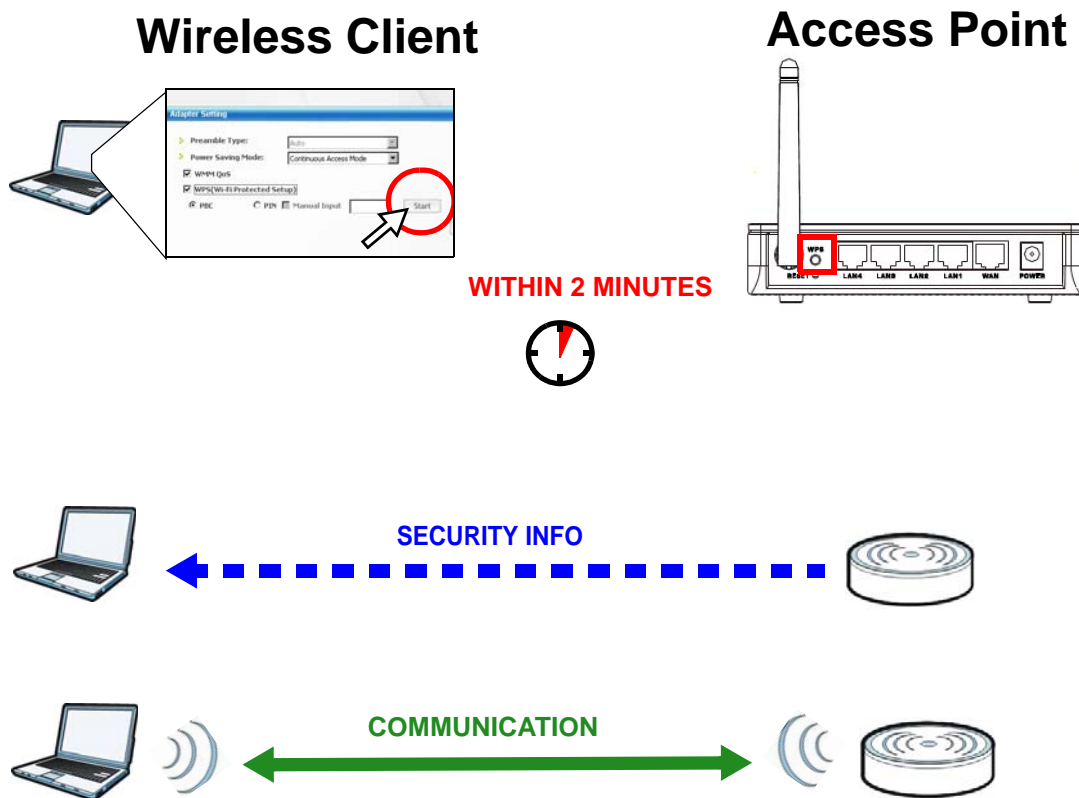
Note: Your NBG4104 has a WPS button located on its back panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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 NBG4104 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 NBG4104 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG4104 and wireless client (the NWD210N in this example).

Figure 17 Example WPS Process: PBC Method



8.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both NBG4104's configuration interface and the client's utilities.

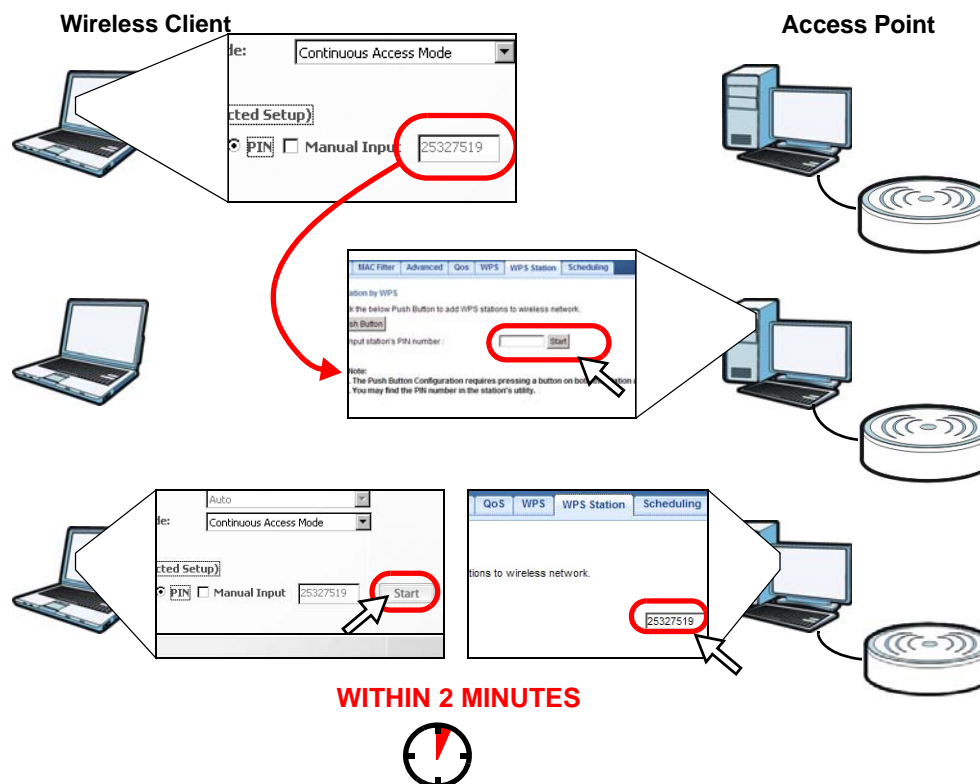
- 1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
- 2 Enter the PIN number to the **PIN** field in the **Configuration > Networking > Wireless LAN > WPS Station** screen on the NBG4104.

- Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG4104's **WPS Station** screen within two minutes.

The NBG4104 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 NBG4104 securely.

The following figure shows you the example to set up wireless network and security on NBG4104 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 18 Example WPS Process: PIN Method



8.3 Configure Wireless Security without WPS

This example shows you how to configure wireless security settings with the following parameters on your NBG4104.

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

Follow the steps below to configure the wireless settings on your NBG4104.

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 21](#)).

- 1 Open the **Configuration > Networking > Wireless LAN > General** screen in the NBG4104's Web Configurator.
- 2 In the **Wireless Setup** section, select the **Wireless LAN** checkbox.
- 3 Enter **SSID_Example** as the SSID and select **Channel-06** as the channel.
- 4 Click **Apply** to save your SSID settings.
- 5 In the same screen, go to the **Security** section and set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

The screenshot shows the 'General' tab of the 'Wireless LAN' configuration page. The 'Wireless Setup' section includes a checked 'Wireless LAN' checkbox, a 'Network Name(SSID)' field with 'SSID_Example', and three 'Enable Network Name(SSID)' options for NBG4104_1, NBG4104_2, and NBG4104_3. The 'Channel Selection' dropdown is set to 'Channel-06 2437MHz'. The 'Security' section shows 'SSID' as 'SSID_Example', 'Security Mode' as 'WPA-PSK', and a 'Pass Phrase' field containing 'ThisismyWPA-PSKpre-shared'. A note states: 'Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled.' The 'WPA' section shows 'WPA Algorithms' with 'AES' selected and 'Pass Phrase' as 'ThisismyWPA-PSKpre-shared'. 'Key Renewal Interval' is set to 3600 seconds. 'Apply' and 'Reset' buttons are at the bottom.

- 6 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**.

The screenshot shows the 'Status' page. On the left, 'Device Information' includes 'WLAN Information' with fields: MAC Address (CA:6C:87:AF:69:38), Radio (On), Name(SSID) (SSID_Example), Channel (6), Operating Channel (6), Security Mode (WPAPSK), 802.11 Mode (802.11 b/g/n mixed mode), and WPS (N/A). On the right, 'Interface Status' table shows:

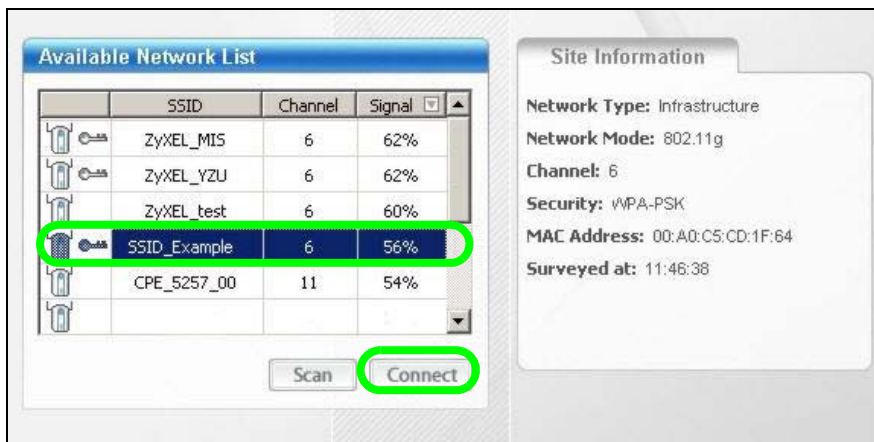
| Interface | Status | Rate |
|-----------|--------|---------|
| WAN | Up | 100Mbps |
| LAN1 | Down | N/A |
| LAN2 | Up | 100Mbps |
| LAN3 | Down | N/A |
| LAN4 | Down | N/A |
| WLAN | On | 150 M |

Below the table is a 'Summary' section with links for 'DHCP Table (Details...)', 'Packet Statistics (Details...)', and 'WLAN Station Status (Details...)'.

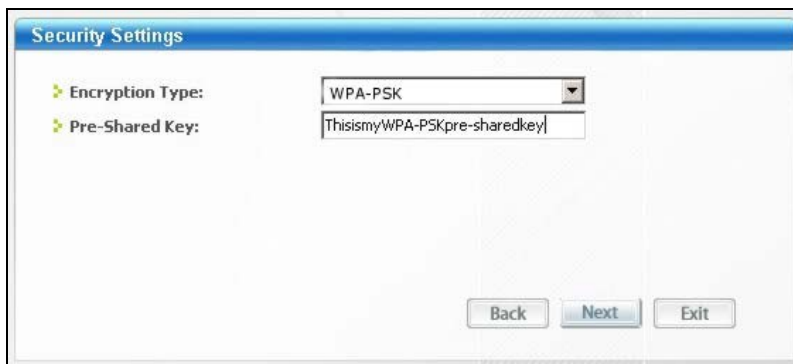
8.3.1 Configure Your Notebook

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

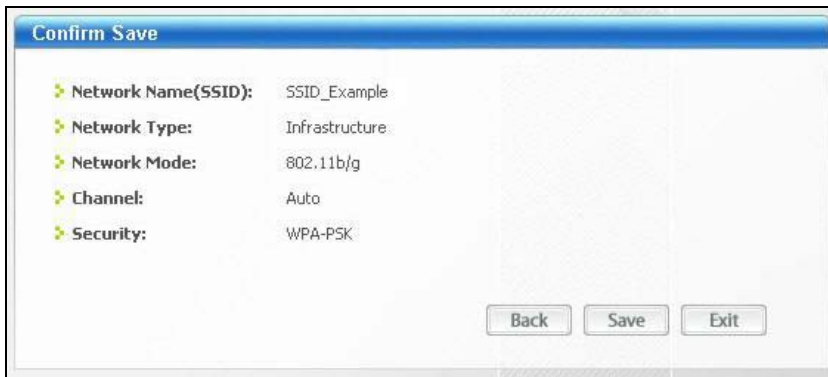
- 1 The NBG4104 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.
- 2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless 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**.



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



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



- 7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see [Chapter 24 Troubleshooting](#) section of this User's Guide.



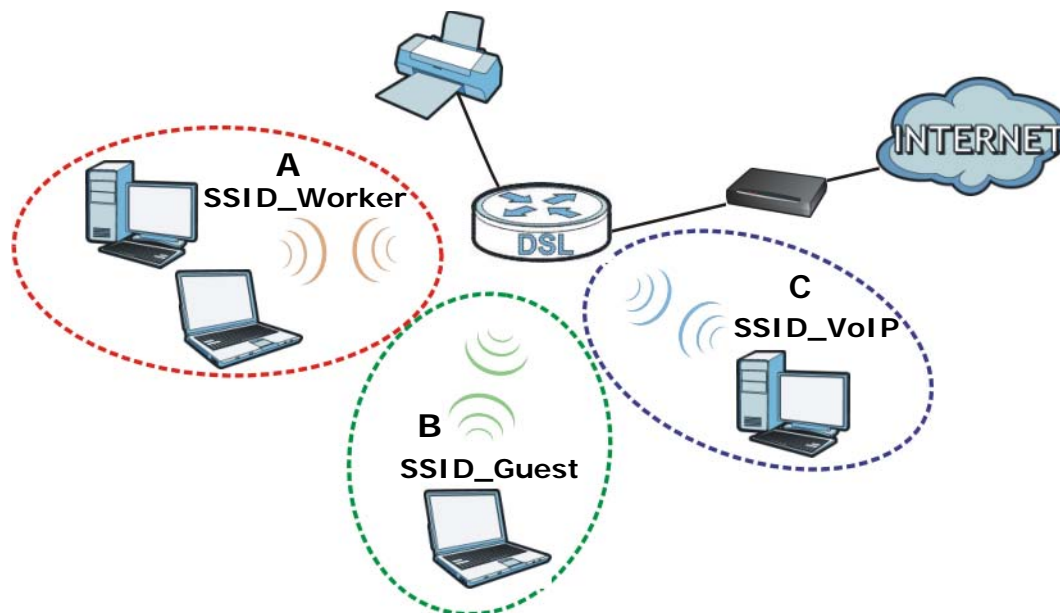
If your connection is successful, open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

8.4 Using Multiple SSIDs on the NBG4104

You can configure more than one SSID on a NBG4104 when it is operating in access point or universal repeater mode. This allows you to configure multiple independent wireless networks on the NBG4104 as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, wireless security type and MAC filtering settings. That is, each SSID on the NBG4104 represents a different access point/wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the NBG4104 (such as a printer). You can allow communication between wireless clients of different SSIDs in the **Configuration > Network > Wireless LAN > General** screen. See [Section 9.4 on page 58](#) for more information.

For example, you may set up three wireless networks (A, B and C) in your office. A is for workers, B is for guests and C is specific to a VoIP device in the meeting room.



8.4.1 Configuring Security Settings of Multiple SSIDs

This example shows you how to configure the SSIDs with the following parameters on your NBG4104 (in access point mode).

| SSID | SECURITY TYPE | KEY | MAC FILTERING |
|-------------|----------------------------|---------------------------------|----------------------------|
| SSID_Worker | WPA2-PSK WPA Compatible | DoNotStealMyWirelessNet work | Disable |
| SSID_Guest | Static WEP 128bit | keyexample123 | Disable |
| SSID_VoIP | WPA-PSK | VoIPOnly12345678 | Allow 00:A0:C5:01:23:45 |

- 1 Connect your computer to the LAN port of the NBG4104 using an Ethernet cable.
- 2 The default IP address of the NBG4104 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix D on page 185](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.
- 5 Enter "1234" (default) as the password and click **Login**.
- 6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

- 7 Go to **Configuration > Networking > Wireless LAN > General**. In the **Wireless Setup** section, enable and enter the SSIDs as the parameters above. Click **Apply** to save the SSID settings.
- 8 Then go to the **Security** section to configure security settings for each SSID. Select **SSID_Worker** from the **SSID** drop-down list. Select **WPA2-PSK** as the **Security Mode**. Enter the **Pass Phrase**. Click **Apply**. Repeat this step and setup security settings for other SSIDs according to the parameters above.

General | MAC Filter | Advanced | Qos | WPS | WPS Station | Scheduling

Wireless Setup

Wireless LAN

Network Name(SSID): Hide SSID

Enable Network Name(SSID 1): Hide SSID

Enable Network Name(SSID 2): Hide SSID

Enable Network Name(SSID 3): Hide SSID

Channel Selection: Auto Channel Selection

Operating Channel:

Security

SSID:

Security Mode:

Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled.

WPA

WPA Compatible

WPA Algorithms: TKIP AES TKIP or AES

Pass Phrase:

Key Renewal Interval: seconds (0 ~ 4194303)

- 9 Click the **MAC Filter** tab to configure MAC filtering for the **SSID_VoIP** wireless network. Select **SSID_VoIP** from the **SSID** drop-down list and select **Allow** in the **Policy** field. Enter the VoIP device's MAC address in the **Add a station Mac Address** field and click **Apply** to allow only the VoIP device to associate with the NBG4104 using this SSID.

General | MAC Filter | Advanced | Qos | WPS | WPS Station | Scheduling

MAC Address Filter

SSID:

Policy:

Add a station Mac Address:

Application List

| MAC Filter Summary | | | |
|--------------------|-------------|--------|-------------|
| Delete | MAC Address | Delete | MAC Address |

PART II

Technical Reference

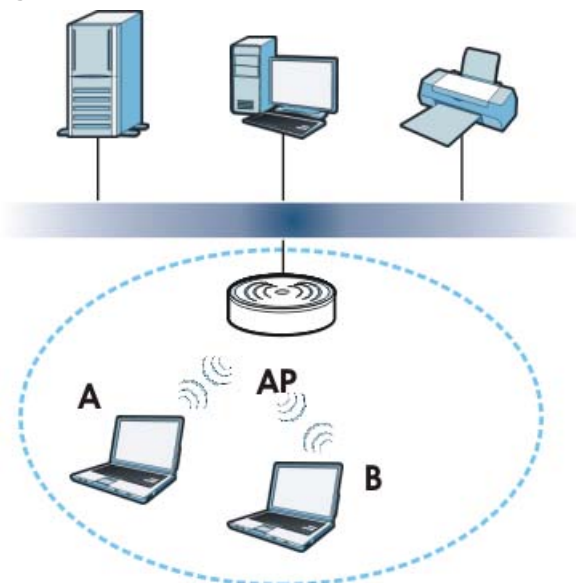
Wireless LAN

9.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG4104. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 19 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 NBG4104 is the AP.

9.2 What You Can Do

- Use the **General** screen to enter the SSID, select the channel, and configure wireless security ([Section 9.4 on page 58](#)).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG4104 ([Section 9.6 on page 62](#)).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold ([Section 9.7 on page 63](#)).
- Use the **QoS** screen to ensure Quality of Service (QoS) in your wireless network ([Section 9.8 on page 65](#)).

- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually ([Section 9.9 on page 65](#)).
- Use the **WPS Station** screen to add a wireless station using WPS ([Section 9.10 on page 66](#)).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off ([Section 9.11 on page 67](#)).

9.3 What You Should Know

Every wireless network must follow these basic guidelines.

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

Wireless Security Overview

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

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.

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

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.

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.

User Authentication

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

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

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

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

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


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

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 [page 57](#) for information about this.)

Table 14 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-PSK** in your NBG4104, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** (depending on the type of wireless network login) and select the **WPA Compatible** option in the NBG4104.

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.

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 8.2 on page 45](#).

9.4 General Wireless LAN Screen

Use this screen to configure the SSID of the wireless LAN and configure the wireless security mode. The screen varies depending on what you select in the **Security Mode** field.

Note: If you are configuring the NBG4104 from a computer connected to the wireless LAN and you change the NBG4104'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 NBG4104's new settings.

Click **Configuration > Networking > Wireless LAN** to open the **General** screen.

Figure 20 Configuration > Networking > Wireless LAN > General

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

Table 15 Configuration > Networking > Wireless LAN > General

| LABEL | DESCRIPTION |
|------------------------|--|
| Wireless LAN | This shows whether the wireless LAN is ON or OFF . You can enable or disable the wireless LAN by using the WLAN switch located on the back panel of the NBG4104. |
| Network Name(SSID) | The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN. |
| Enable | Select this to activate the wireless network. |
| Network Name(SSID 1~3) | You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the NBG4104. This allows you to use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point. |
| 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 | This option is only available if Auto Channel Selection is disabled. Note: According to the FCC regulation, users can only select the channels 1-11 for 802.11b/g/n-HT20 and 3-9 channels for 802.11n-HT40 mode. The other channels that out of the permission above will be disabled from the channel selection. |
| Operating Channel | This displays the channel the NBG4104 is currently using. |
| SSID | Select a wireless LAN for which to configure security settings. The security settings only apply to the selected wireless LAN. |
| Security Mode | Choose the security mode from the drop-down list box. See Section 9.5 on page 60 for more information on wireless security settings. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| 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.

9.5 Wireless Security

Use this part of the **General** screen to select the wireless security mode. Click **Network > Wireless LAN** to open the **General** screen. The screen varies depending on what you select in the **Security Mode** field.

9.5.1 No Security

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

Note: If you do not enable any wireless security on your NBG4104, your network is accessible to any wireless networking device that is within range.

Figure 21 Wireless LAN > General: Security: No Security

The following table describes the labels in this screen.

Table 16 Wireless LAN > General: Security: No Security

| LABEL | DESCRIPTION |
|---------------|--|
| SSID | Select a wireless LAN for which to configure security settings. The security settings only apply to the selected wireless LAN. |
| Security Mode | Choose No Security from the drop-down list box. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |

9.5.2 WEP Encryption

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

Your NBG4104 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.

Select **Static WEP** from the **Security Mode** list.

Figure 22 Wireless LAN > General: Security: Static WEP

Security

SSID :

Security Mode :

Note: WPA-PSK and WPA2-PSK can be configured when WPS enabled.

Wire Equivalence Protection (WEP)

Default Key :

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Note: Key 1~4 can accept 64 bits (5 characters in ASCII or 10 characters in Hex) or 128 bits (13 characters in ASCII or 26 characters in Hex) format separately.

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

Table 17 Wireless LAN > General: Security: Static WEP

| LABEL | DESCRIPTION |
|--------------------|---|
| SSID | Select a wireless LAN for which to configure security settings. The security settings only apply to the selected wireless LAN. |
| Security Mode | Select Static WEP to enable data encryption. |
| Default Key | Select a WEP Key as your default key. |
| WEP Key 1 to Key 4 | The WEP keys are used to encrypt data. Both the NBG4104 and the wireless stations must use the same WEP key for data transmission. Select ASCII to enter ASCII characters or select Hex to enter hexadecimal characters as WEP key. You must configure at least one key, only one key can be activated at any one time. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |

9.5.3 WPA-PSK/WPA2-PSK

Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 23 Wireless LAN > General: Security: WPA-PSK/WPA2-PSK

The screenshot shows the configuration page for Wireless LAN security. Under the 'Security' section, the SSID is set to 'NBG4104' and the Security Mode is set to 'WPA2-PSK'. A note indicates that WPA-PSK and WPA2-PSK can be configured when WPS is enabled. Under the 'WPA' section, the 'WPA Compatible' checkbox is unchecked. The 'WPA Algorithms' section has three radio buttons: 'TKIP' (unchecked), 'AES' (checked), and 'TKIP or AES' (unchecked). The 'Pass Phrase' is set to '12345678' and the 'Key Renewal Interval' is set to '3600' seconds. At the bottom right, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 18 Wireless LAN > General: Security: WPA-PSK/WPA2-PSK

| LABEL | DESCRIPTION |
|----------------------|--|
| SSID | Select a wireless LAN for which to configure security settings. The security settings only apply to the selected wireless LAN. |
| Security Mode | Select WPA-PSK or WPA2-PSK to enable data encryption. |
| WPA Compatible | This field appears when you choose WPA2-PSK as the Security Mode . Check this field to allow wireless devices using WPA-PSK security mode to connect to your NBG4104. |
| WPA Algorithms | Select the encryption type (TKIP , AES , or TKIP or AES) for data encryption. Select TKIP if your wireless clients can all use TKIP. Select AES if your wireless clients can all use AES. Select TKIP or AES to allow the wireless clients to use either TKIP or AES. |
| Pass Phrase | WPA-PSK/WPA2-PSK uses a simple common password for authentication. Type a pass phrase from 8 to 63 case-sensitive keyboard characters. |
| Key Renewal Interval | This is the rate at which the AP sends a new group key out to all clients. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |

9.6 MAC Filter

The MAC filter screen allows you to configure the NBG4104 to give exclusive access to devices (Allow) or exclude devices from accessing the NBG4104 (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 NBG4104's MAC filter settings, click **Configuration > Networking > Wireless LAN > MAC Filter**. The screen appears as shown.

Figure 24 Configuration > Networking > Wireless LAN > MAC Filter

The following table describes the labels in this menu.

Table 19 Configuration > Networking > Wireless LAN > MAC Filter

| LABEL | DESCRIPTION |
|---------------------------|--|
| SSID | Select the SSID for which you want to configure MAC filtering. |
| Policy | Define the filter action for the list of MAC addresses in the MAC Address table. Select Disable to deactivate the MAC filtering rule you configure below. Select Allow to permit access to the NBG4104, MAC addresses not listed will be denied access to the NBG4104. Select Reject to block access to the NBG4104, MAC addresses not listed will be allowed to access the NBG4104 |
| Add a station Mac Address | Enter the MAC addresses of the wireless station that are allowed or denied access to the NBG4104 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. Click Add . |
| Delete | Click the delete icon to remove the MAC address from the list. |
| MAC Address | This is the MAC address of the wireless station that are allowed or denied access to the NBG4104. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |

9.7 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as the output power, RTS/CTS Threshold and high-throughput physical mode settings.

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

Figure 25 Configuration > Networking > Wireless LAN > Advanced

The following table describes the labels in this screen.

Table 20 Configuration > Networking > Wireless LAN > Advanced

| LABEL | DESCRIPTION |
|---|--|
| RTS/CTS Threshold | Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 256 and 2432. |
| Fragmentation Threshold | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between 256 and 2346 . |
| Enable Intra-BSS Traffic | A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client 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. |
| Output Power | Set the output power of the NBG4104 in this field. If there is a high density of APs in an area, decrease the output power of the NBG4104 to reduce interference with other APs. Select one of the following 100% , 90% , 75% , 50% , 25% or 10% . See the product specifications for more information on your NBG4104's output power. |
| HT (High Throughput) Physical Mode - Use the fields below to configure the 802.11 wireless environment of your NBG4104. | |
| Channel Bandwidth | Select the channel bandwidth you want to use for your wireless network. It is recommended that you select 20/40 (20/40 MHz). Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood. |
| Guard Interval | Select Auto to increase data throughput. However, this may make data transfer more prone to errors. Select Long to prioritize data integrity. This may be because your wireless network is busy and congested or the NBG4104 is located in an environment prone to radio interference. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |

9.8 Quality of Service (QoS) Screen

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

Click **Configuration > Networking > Wireless LAN > QoS**. The following screen appears.

Figure 26 Configuration > Networking > Wireless LAN > QoS

The screenshot shows a web interface with a navigation bar at the top containing tabs: General, MAC Filter, Advanced, Qos, WPS, WPS Station, and Scheduling. The 'Qos' tab is selected. Below the navigation bar, the page title is 'WMM Configuration'. There is a single checkbox labeled 'Enable WMM QoS' which is checked. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 21 Configuration > Networking > Wireless LAN > QoS

| LABEL | DESCRIPTION |
|----------------|--|
| Enable WMM QoS | Check this to have the NBG4104 automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. |
| Apply | Click Apply to save your changes to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |

9.9 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 **Configuration > Networking > Wireless LAN > WPS** tab.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the NBG4104.

Figure 27 Configuration > Networking > Wireless LAN > WPS

The screenshot shows a web interface with a navigation bar at the top containing tabs: General, MAC Filter, Advanced, Qos, WPS, WPS Station, and Scheduling. The 'WPS' tab is selected. Below the navigation bar, the page title is 'WPS Setup'. There is a checked checkbox labeled 'Enable WPS'. Below it is a 'PIN Number' field containing the value '14957369' and a 'Generate' button. A horizontal line separates the setup section from the status section. The status section has a 'Status' field with the value 'Unconfigured' and a 'Release Configuration' button. Below that are three rows of status information: '802.11 Mode: 11b/g/n', 'SSID: NBG4104', and 'Security: WPA2-PSK'. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 22 Configuration > Networking > Wireless LAN > WPS

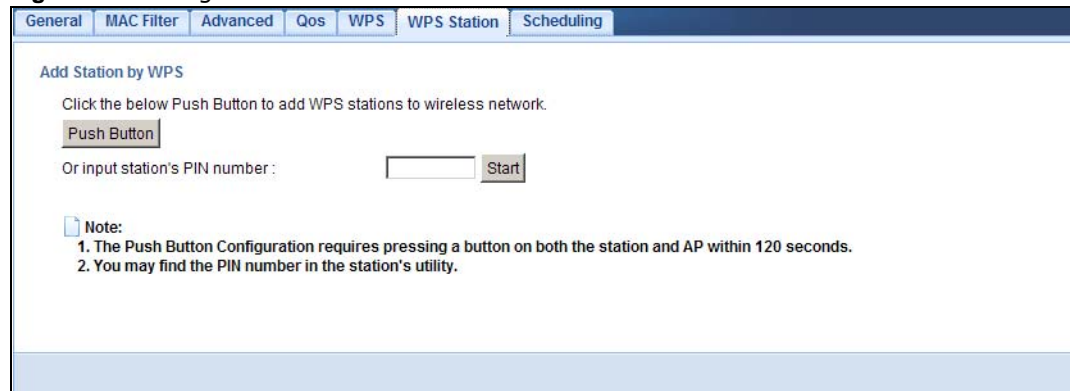
| LABEL | DESCRIPTION |
|-----------------------|---|
| Enable WPS | Select this to enable the WPS feature. |
| PIN Number | This displays a PIN number last time system generated. Click Generate to generate a new PIN number. |
| Status | This displays Configured when the NBG4104 has connected to a wireless 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 NBG4104 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 NBG4104. |
| 802.11 Mode | This is the 802.11 mode used. Only compliant WLAN devices can associate with the NBG4104. |
| SSID | This is the name of the wireless network (the NBG4104's first SSID). |
| Security | This is the type of wireless security employed by the network. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |

9.10 WPS Station Screen

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

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 28 Configuration > Wireless LAN > WPS Station



The following table describes the labels in this screen.

Table 23 Configuration > Networking > Wireless LAN > WPS Station

| LABEL | DESCRIPTION |
|-------------------------------|---|
| Push Button | Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. 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. 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. |

9.11 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 **Configuration > Networking > Wireless LAN > Scheduling** tab.

Figure 29 Configuration > Networking > Wireless LAN > Scheduling

Wireless LAN Scheduling

Enable Wireless LAN Scheduling

| WLAN status | Day | At the following times (24-Hour Format) |
|---|-----------------------------------|---|
| <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) |

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

Apply

The following table describes the labels in this screen.

Table 24 Configuration > Networking > Wireless LAN > Scheduling

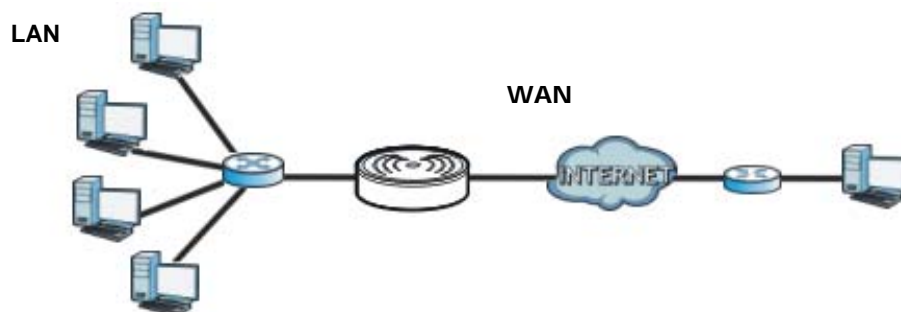
| LABEL | DESCRIPTION |
|---|--|
| Enable Wireless LAN Scheduling | Select this to enable Wireless LAN scheduling. |
| WLAN Status | Select On or Off to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the Day and For the following times fields. |
| Day | Select 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 For the following times field. |
| At 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 on between the two times you enter in these fields. If you have chosen Off earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. |
| Apply | Click Apply to save your changes back to the NBG4104. |

10.1 Overview

This chapter discusses the NBG4104's **WAN** screens. Use these screens to configure your NBG4104 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 30 LAN and WAN



10.2 What You Can Do

- Use the **Management WAN** screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses ([Section 10.4 on page 72](#)).
- Use the **Advanced** screen to enable multicasting and auto-IP-change ([Section 10.5 on page 79](#)).

10.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your NBG4104.

10.3.1 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 NBG4104, which makes it accessible from an outside network. It is used by the NBG4104 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG4104 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 NBG4104 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 NBG4104'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.

Maximum Transmission Unit

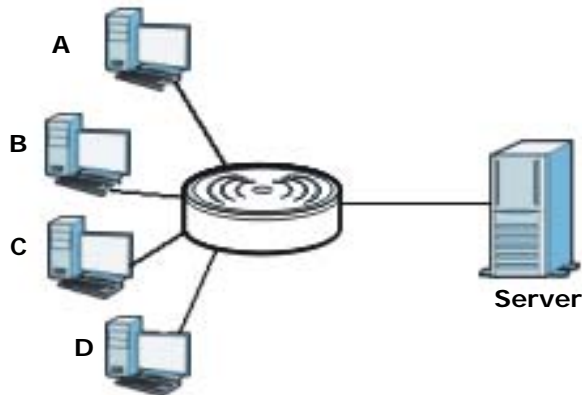
A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network. The Transmission Control Protocol

(TCP) uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled.

10.3.2 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 31 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 NBG4104 supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

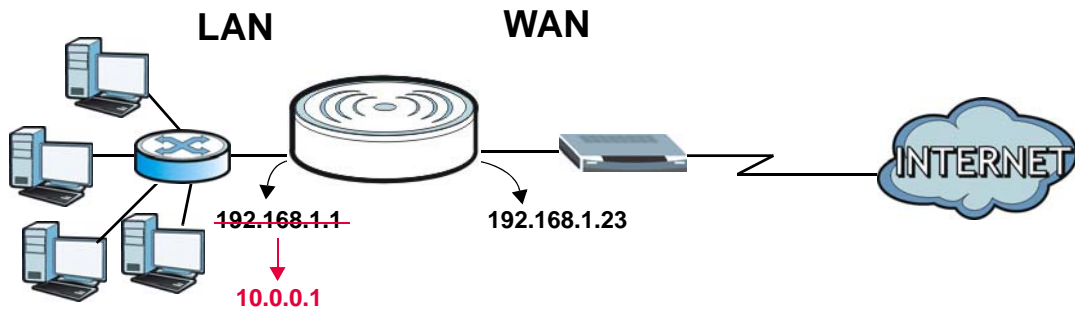
At start up, the NBG4104 queries all directly connected networks to gather group membership. After that, the NBG4104 periodically updates this information. IP multicasting can be enabled/disabled on the NBG4104 LAN and/or WAN interfaces in the Web Configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

Auto-IP-Change

When the NBG4104 gets a WAN IP address which is in the same subnet as the LAN IP address 192.168.1.1, Auto-IP-Change allows the NBG4104 to change its LAN IP address to 10.0.0.1 automatically. If the NBG4104's original LAN IP address is 10.0.0.1 and the WAN IP address is in

the same subnet, such as 10.0.0.3, the NBG4104 switches to use 192.168.1.1 as its LAN IP address.

Figure 32 Auto-IP-Change



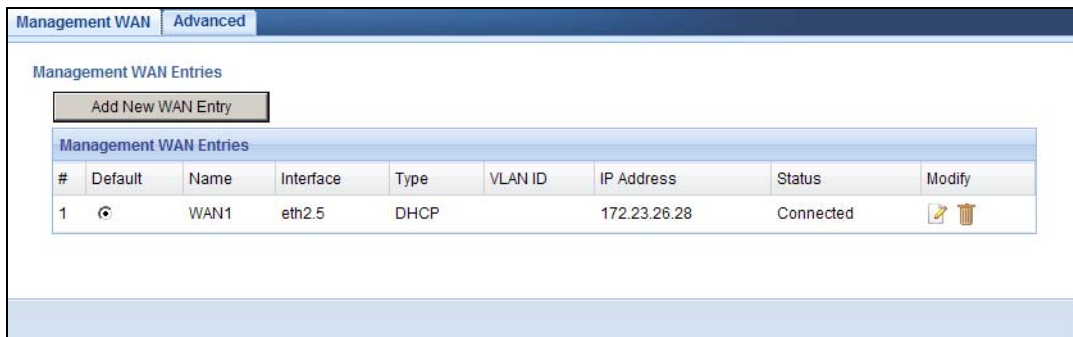
Auto-IP-Change only works under the following conditions:

- The NBG4104 must be in **Router Mode** (see [Chapter 23 on page 150](#) for more information) for Auto-IP-Change to become active.
- The NBG4104 is set to receive a dynamic WAN IP address using the Ethernet or PPPoE connection type.

10.4 Management WAN

Use this screen to view, change, or add your NBG4104’s Internet access settings. Click **Configuration > Networking > WAN**. The following screen opens.

Figure 33 Configuration > Networking > Management WAN



The following table describes the labels in this screen.

Table 25 Configuration > Networking > Management WAN

| LABEL | DESCRIPTION |
|-------------------|---|
| Add New WAN Entry | Click this to create a new WAN interface entry. |
| # | This is the index number of the connection. |
| Default | Select the WAN interface that you want to configure as default. |
| Name | This is the service name of the connection. |
| Interface | This is the interface of the connection. |

Table 25 Configuration > Networking > Management WAN (continued)

| LABEL | DESCRIPTION |
|------------|---|
| Type | This shows the type of interface used by this connection. |
| VLAN ID | This indicates the VLAN ID number assigned to traffic sent through this connection. |
| IP Address | This is the WAN IP address used by this connection. |
| Status | This shows the status of the connection. |
| Modify | Click the Edit icon to configure the connection. Click the Delete icon to delete this connection from the NBG4104. A window displays asking you to confirm that you want to delete the connection. |

10.4.1 Add/Edit Internet Connection

Click the **Add New WAN Entry** in the **Configuration > WAN** screen or the **Edit** icon next to the connection you want to configure. Use this screen to configure a WAN connection. The screen varies depending on the encapsulation you select.

10.4.2 Ethernet Encapsulation

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

Figure 34 Internet Connection: Ethernet Encapsulation

The screenshot shows the configuration interface for a WAN connection using Ethernet encapsulation. The interface is organized into several sections:

- ISP Parameters for Internet Access:** Includes a text field for 'Name' and a dropdown menu for 'Encapsulation' set to 'Ethernet'.
- WAN IP Address Assignment:** Features two radio buttons: 'Get automatically from ISP (Default)' (selected) and 'Use Fixed IP Address'. Below are input fields for 'IP Address', 'IP Subnet Mask', and 'Gateway IP Address'. The 'MTU Size' is set to 1500, with a note '(512 <= MTU value <= 1500)'.
- WAN DNS Assignment:** Contains two rows, each with a dropdown menu set to 'From ISP' and an input field for the DNS server address, both set to '0.0.0.0'.
- WAN MAC Address:** Includes three radio buttons: 'Factory default' (selected), 'Clone the computer's MAC address - IP Address', and 'Set WAN MAC Address' with the value 'C8:6C:87:99:69:2F'.
- VLAN Settings:** Has two checkboxes: 'Enable VLAN' (unchecked) and 'Ignore WAN VLAN ID when tag frame receive from LAN side.' (checked). Below are input fields for 'VLAN ID' and '802.1P' (set to 0).

At the bottom of the form are three buttons: 'Apply', 'Reset', and 'Cancel'.

The following table describes the labels in this screen.

Table 26 Internet Connection: Ethernet Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Name | Enter a service name of the connection. |
| Encapsulation | You must choose the Ethernet option when the WAN port is used as a regular Ethernet. |
| WAN IP Address Assignment | |
| Get automatically from ISP (Default) | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use Fixed IP Address | Select this option If the ISP assigned a fixed IP address. |
| IP Address | Enter your WAN IP address in this field if you selected 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. |
| MTU Size | Enter the MTU (Maximum Transfer Unit) size for this traffic. |
| WAN DNS Assignment | |
| First DNS Server Second DNS Server | If you select Get automatically from ISP (Default) in the WAN IP Address Assignment section, this field will automatically be set to From ISP . The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you select Use Fixed IP Address in the WAN IP Address Assignment section, this field will automatically be set to User-Defined . Enter the DNS server's IP address in the field to the right. |
| WAN MAC Address | The MAC address section allows users to configure the WAN port's MAC address by either using the NBG4104'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. |
| 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 NBG4104. |
| VLAN Settings | |
| Enable VLAN | Select this to add the VLAN tag (specified in the VLAN ID field below) to the outgoing traffic through this connection. |
| Ignore WAN VLAN ID when tag frame receive from LAN side | Select this to ignore VLAN ID tagging if the tag frame is from the LAN. |
| VLAN ID | Type the VLAN ID number (from 1 to 4094) for traffic through this connection. |
| 802.1P | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

10.4.3 PPPoE Encapsulation

The NBG4104 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 NBG4104 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG4104 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

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

Figure 35 Internet Connection: PPP over Ethernet Encapsulation

The following table describes the labels in this screen.

Table 27 Internet Connection: PPP over Ethernet Encapsulation

| LABEL | DESCRIPTION |
|------------------------------------|--|
| ISP Parameters for Internet Access | |
| Encapsulation | Select PPP over Ethernet if you connect to your Internet via dial-up. |
| Service Name | Type the name of your PPPoE service here. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |

Table 27 Internet Connection: PPP over Ethernet Encapsulation (continued)

| LABEL | DESCRIPTION |
|---|---|
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |
| PPPoE Passthrough | In addition to the NBG4104's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the NBG4104. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP. |
| MTU Size | Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your NBG4104 can receive and process. |
| Nailed-Up Connection | Select Nailed-Up Connection if you do not want the connection to time out. |
| Idle Timeout (sec) | This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. |
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use Fixed IP Address | Select this option If the ISP assigned a fixed IP address. |
| IP Address | Enter the static IP address provided by your ISP. |
| IP Subnet Mask | Enter the subnet mask provided by your ISP. |
| Gateway IP Address | Enter the gateway IP address provided by your ISP. |
| WAN DNS Assignment | |
| First DNS Server Second DNS Server | Select From ISP if your ISP dynamically assigns DNS server information (and the NBG4104's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. 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 NBG4104'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. |
| Set WAN MAC Address | Select this option and enter the MAC address you want to use. |
| VLAN Settings | |
| Enable VLAN | Select this to add the VLAN tag (specified in the VLAN ID field below) to the outgoing traffic through this connection. |

Table 27 Internet Connection: PPP over Ethernet Encapsulation (continued)

| LABEL | DESCRIPTION |
|---|--|
| Ignore WAN VLAN ID when tag frame receive from LAN side | Select this to ignore VLAN ID tagging if the tag frame is from the LAN. |
| VLAN ID | Type the VLAN ID number (from 1 to 4094) for traffic through this connection. |
| 802.1P | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

10.4.4 Bridge Encapsulation

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

Figure 36 Internet Connection: Bridge Encapsulation

The following table describes the labels in this screen.

Table 28 Internet Connection: Bridge Encapsulation

| LABEL | DESCRIPTION |
|------------------------------------|--|
| ISP Parameters for Internet Access | |
| Name | Enter a service name of the connection. |
| Encapsulation | Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select Bridge , you cannot use routing functions, such as DHCP server. |
| VLAN Settings | |
| Enable VLAN | Select this to add the VLAN tag (specified in the VLAN ID field below) to the outgoing traffic through this connection. |

Table 28 Internet Connection: Bridge Encapsulation (continued)

| LABEL | DESCRIPTION |
|---|--|
| Ignore WAN VLAN ID when tag frame receive from LAN side | Select this to ignore VLAN ID tagging if the tag frame is from the LAN. |
| VLAN ID | Type the VLAN ID number (from 1 to 4094) for traffic through this connection. |
| 802.1P | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to reload the previous configuration for this screen. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

10.5 Advanced WAN Screen

Use this screen to enable **Multicast** and enable **Auto-IP-Change** mode.

To change your NBG4104's advanced WAN settings, click **Configuration > Networking > WAN > Advanced**. The screen appears as shown.

Figure 37 Configuration > Networking > WAN > Advanced

The following table describes the labels in this screen.

Table 29 Configuration > Networking > WAN > Advanced

| LABEL | DESCRIPTION |
|---------------------------|---|
| Multicast Setup | |
| Multicast | Check this to enable multicasting. This applies to traffic routed from the WAN to the LAN. Leaving this blank may cause incoming traffic to be dropped or sent to all connected network devices. |
| Auto-Subnet Configuration | |

Table 29 Configuration > Networking > WAN > Advanced (continued)

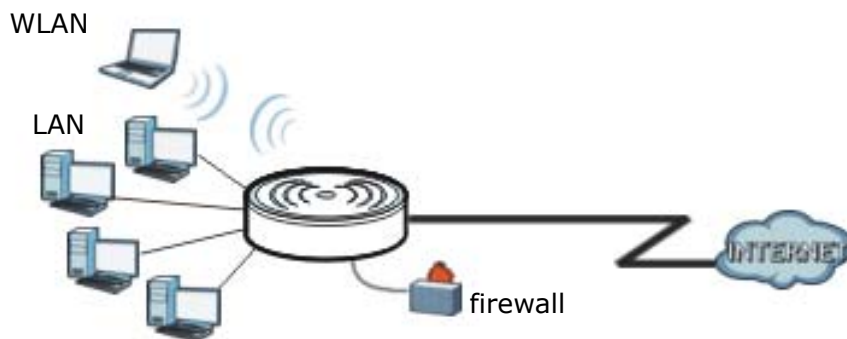
| LABEL | DESCRIPTION |
|----------------------------|--|
| None | Select this option to have the NBG4104 do nothing when it gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) or in the same subnet as the LAN IP address. |
| Enable Auto-IP-Change mode | Select this option to have the NBG4104 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG4104 gets a dynamic WAN IP address in the same subnet as the LAN IP address 192.168.1.1 or 10.0.0.1. The NAT, DHCP server and firewall functions on the NBG4104 are still available in this mode. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

11.1 Overview

This chapter describes how to configure LAN settings.

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

Figure 38 LAN Example



The LAN screens can help you manage IP addresses.

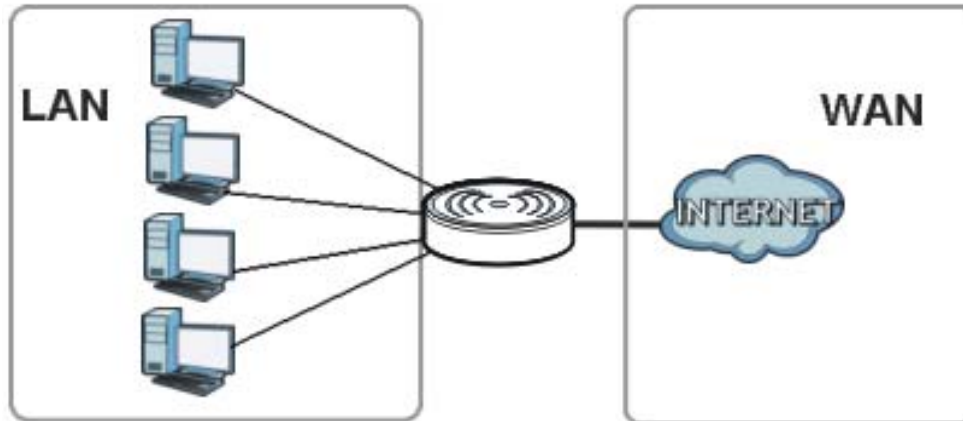
11.2 What You Can Do

- Use the **IP** screen to change the IP address for your NBG4104 ([Section 11.4 on page 83](#)).
- Use the **IP Alias** screen to have the NBG4104 apply IP alias to create LAN subnets ([Section 11.5 on page 83](#)).

11.3 What You Need To Know

The actual physical connection determines whether the NBG4104 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 39 LAN and WAN IP Addresses



The LAN parameters of the NBG4104 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.

11.3.1 IP Pool Setup

The NBG4104 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 NBG4104 itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, T, web, etc., that you may have.

11.3.2 LAN TCP/IP

The NBG4104 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

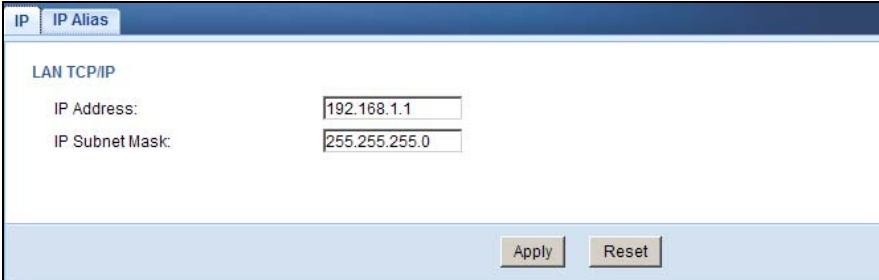
11.3.3 IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The NBG4104 supports three logical LAN interfaces via its single physical Ethernet interface with the NBG4104 itself as the gateway for each LAN network.

11.4 LAN IP Screen

Use this screen to change the IP address for your NBG4104. Click **Configuration > Networking > LAN > IP**.

Figure 40 Configuration > Networking > LAN > IP



The following table describes the labels in this screen.

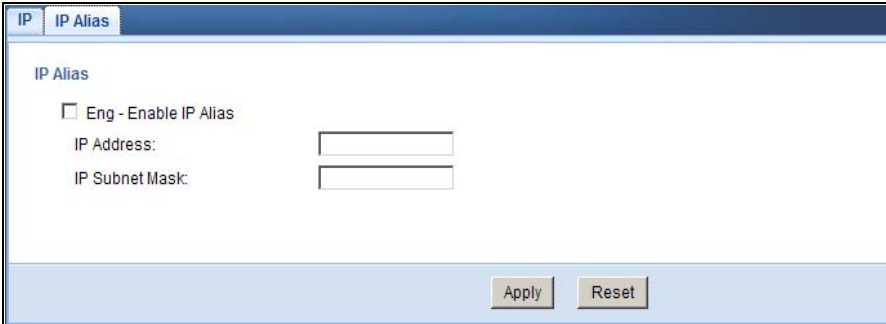
Table 30 Configuration > Networking > LAN > IP

| LABEL | DESCRIPTION |
|----------------|--|
| IP Address | Type the IP address of your NBG4104 in dotted decimal notation. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your NBG4104 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 NBG4104. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

11.5 IP Alias Screen

Use this screen to have the NBG4104 apply IP alias to create LAN subnets. Click **Configuration > Networking > LAN > IP Alias**.

Figure 41 Configuration > Networking > LAN > IP Alias



The following table describes the labels in this screen.

Table 31 Configuration > Networking > LAN > IP Alias

| LABEL | DESCRIPTION |
|-----------------|--|
| Enable IP Alias | Check this to enable IP alias. |
| IP Address | Type the IP alias address of your NBG4104 in dotted decimal notation. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your NBG4104 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 NBG4104. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

DHCP Server

12.1 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 NBG4104's LAN as a DHCP server or disable it. When configured as a server, the NBG4104 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.

12.2 What You Can Do

- Use the **General** screen to enable the DHCP server ([Section 12.4 on page 86](#)).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 12.5 on page 87](#)).

12.3 What You Need To Know

The following terms and concepts may help as you read through this chapter.

MAC Addresses

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.

12.4 The DHCP General Screen

Use this screen to enable the DHCP server. Click **Configuration > Networking > DHCP Server**. The **General** screen displays.

Figure 42 Configuration > Networking > DHCP Server > General

The screenshot shows a web-based configuration interface for a DHCP server. At the top, there are two tabs: 'General' (which is active) and 'Advanced'. Below the tabs, the section is titled 'DHCP Setup'. There are three main configuration items: a checked checkbox labeled 'Enable DHCP Server', a text input field for 'IP Pool Starting Address' containing the value '192.168.1.33', and another text input field for 'Pool Size' containing the value '222'. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 32 Configuration > Networking > DHCP Server > General

| LABEL | DESCRIPTION |
|--------------------------|--|
| Enable DHCP Server | Select the checkbox to enable 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 NBG4104 acting as a DHCP server. When configured as a server, the NBG4104 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 NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

12.5 The DHCP 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 NBG4104 sends to the DHCP clients.

To change your NBG4104's static DHCP settings, click **Configuration > Networking > DHCP Server > Advanced**. The following screen displays.

Figure 43 Configuration > Networking > DHCP Server > Advanced

The screenshot shows the 'Advanced' tab of the DHCP Server configuration. It features a 'Static DHCP Table' with 8 rows. Each row has a '#' column, a 'MAC Address' column with a text input field containing '00:00:00:00:00:00', and an 'IP Address' column with a text input field containing '0.0.0.0'. Below the table is the 'DNS Server' section, which includes 'DNS Servers Assigned by DHCP Server'. The 'First DNS Server' is set to 'DNS Relay' with a dropdown arrow and a text input field containing '0.0.0.0'. The 'Second DNS Server' is set to 'None' with a dropdown arrow and a text input field containing '0.0.0.0'. At the bottom of the screen are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 33 Configuration > Networking > 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 NBG4104 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG4104 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 sever on your LAN, or else the computers must have their DNS server addresses manually configured. |

Table 33 Configuration > Networking > DHCP Server > Advanced (continued)

| LABEL | DESCRIPTION |
|---------------------------------------|--|
| First DNS Server Second DNS Server | <p>Select From ISP if your ISP dynamically assigns DNS server information (and the NBG4104'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 NBG4104 act as a DNS proxy. The NBG4104's LAN IP address displays in the field to the right (read-only). The NBG4104 tells the DHCP clients on the LAN that the NBG4104 itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG4104, the NBG4104 forwards the query to the NBG4104'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 NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

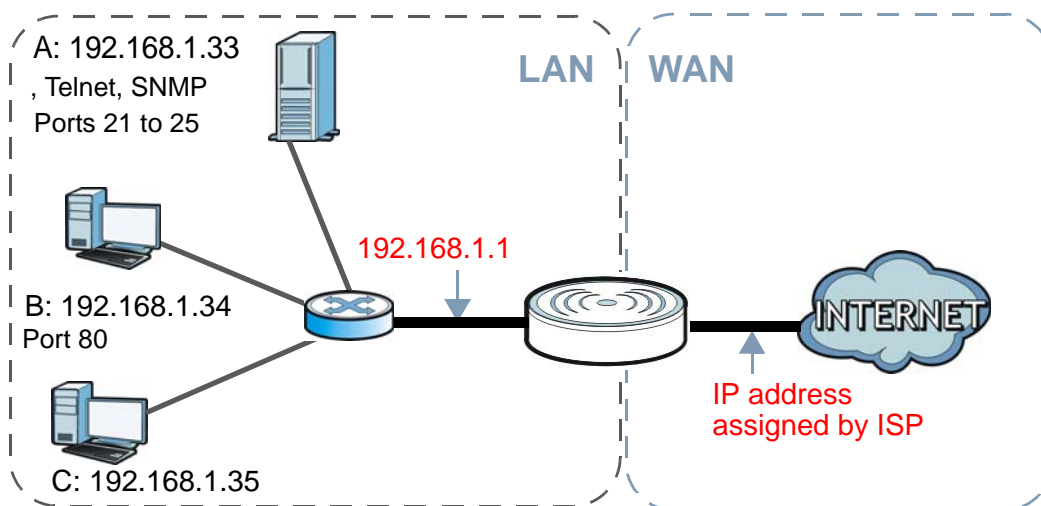
13.1 Overview

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, 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 NBG4104. 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 NBG4104, which is 192.168.1.1.

Figure 44 NAT Example



This chapter discusses how to configure NAT on the NBG4104.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG4104.

13.2 What You Can Do

- Use the **General** screen to enable NAT and set a default server ([Section 13.4 on page 92](#)).
- Use the **Application** screen to change your NBG4104's port forwarding settings ([Section 13.5 on page 92](#)).

13.3 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Inside/Outside

This denotes where a host is located relative to the NBG4104, 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 34 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.

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

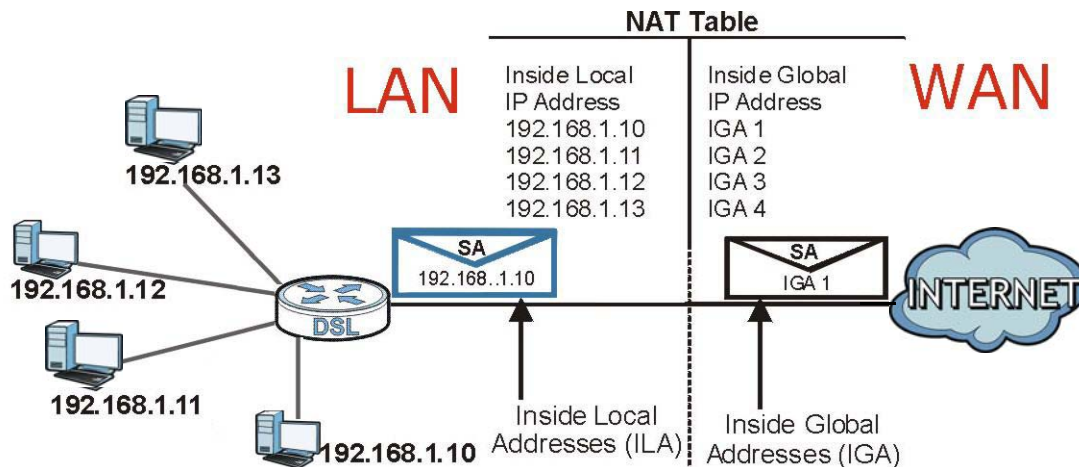
global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

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 NBG4104 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)*.

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 NBG4104 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 45 How NAT Works



13.4 The NAT General Screen

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

Figure 46 Configuration > Networking > NAT > General

The following table describes the labels in this screen.

Table 35 Configuration > Networking > NAT > General

| LABEL | DESCRIPTION |
|------------------------------------|--|
| NAT Setup | |
| Enable Network Address Translation | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT. |
| Default Server Setup | |
| Server IP Address | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the Application screen. If you do not assign a Default Server IP address , the NBG4104 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 NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

13.5 The NAT Application Screen

This screen allows you to define the local servers to which the incoming services will be forwarded. To change your NBG4104's NAT application settings, click **Configuration > Networking > NAT > Application**. The screen appears as shown.

Note: If you do not assign a **Default Server IP address** in the **NAT > General** screen, the NBG4104 discards all packets received for ports that are not specified in this screen or remote management.

Refer to [Appendix F on page 227](#) for port numbers commonly used for particular services.

Figure 47 Configuration > Networking > NAT > Application

The screenshot shows the 'Add Application Rule' configuration page. It includes a 'Service Name' field with a dropdown menu currently set to 'User-Defined'. Below it are 'Local Port Range' and 'Public Port Range' fields, each consisting of two input boxes separated by a tilde (~). The 'Protocol' dropdown is set to 'TCP/UDP'. The 'Service IP Address' field is empty. Below the form is a table titled 'Application Rules Summary' with the following data:

| # | Name | Local | | Public | | Protocol | Service IP Address | Modify |
|---|------|------------|----------|------------|----------|----------|--------------------|--------|
| | | Start Port | End Port | Start Port | End Port | | | |
| 1 | DNS | 53 | - | 53 | - | TCP/UDP | 192.168.1.77 | |

At the bottom of the screen are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 36 Configuration > Networking > NAT > Application

| LABEL | DESCRIPTION |
|----------------------------|--|
| Add Application Rule | |
| Service Name | Select User-Defined and 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 | Enter the start and end port(s) to be forwarded. |
| Public Port Range | |
| Protocol | Select the protocol supported by this service. Choices are TCP/UDP , TCP , or UDP . |
| Server IP Address | Type the inside IP address of the server that receives packets from the port(s) specified in the Port field. |
| Application Rules Summary | |
| # | This is the number of an individual port forwarding server entry. |
| Name | This field displays a name to identify this rule. |
| Local Start Port/End Port | This is the first and last internal port number that identifies a service. |
| Public Start Port/End Port | This is the first and last external port number that identifies a service. |
| Protocol | This is the protocol used by this service. |
| 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. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

14.1 Overview

DDNS services let you use a domain name with a dynamic IP address.

14.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

What is DDNS?

DDNS, or 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 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.

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.

14.3 The DDNS General Screen

To change your NBG4104's DDNS, click **Configuration > Networking > DDNS**. The **General** screen appears as shown.

Figure 48 Configuration > Networking > DDNS > General

The following table describes the labels in this screen.

Table 37 Configuration > Networking > DDNS > General

| 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. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

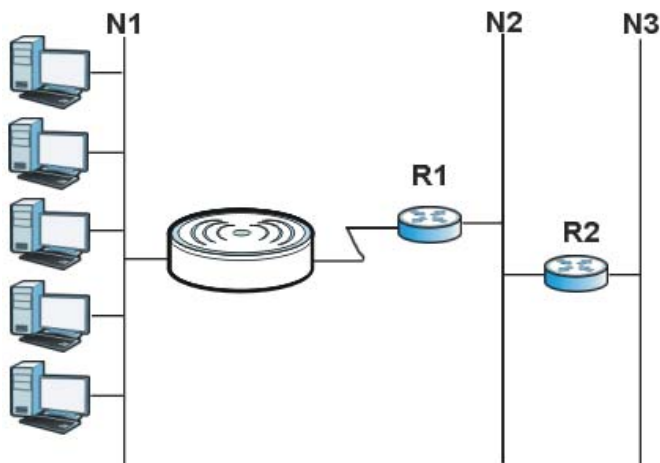
Static Route

15.1 Overview

This chapter shows you how to configure static routes for your NBG4104.

Each remote node specifies only the network to which the gateway is directly connected, and the NBG4104 has no knowledge of the networks beyond. For instance, the NBG4104 knows about network N2 in the following figure through remote node Router 1. However, the NBG4104 is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the NBG4104 about the networks beyond the remote nodes.

Figure 49 Example of Static Routing Topology



15.2 IP Static Route Screen

Click **Configuration > Networking > Static Route** to open the **IP Static Route** screen.

Figure 50 Configuration > Networking > Static Route > IP Static Route

The screenshot shows the 'IP Static Route' configuration interface. It features a 'Static Routing Settings' section with the following fields: 'Route Name', 'Destination IP Address', 'IP Subnet Mask', 'Gateway IP Address', 'Metric', and 'Interface' (a dropdown menu currently showing 'LAN'). Below these fields is an 'Add Rule' button. Underneath is an 'Application Rules Summary' table with the following columns: 'No.', 'Active', 'Name', 'Destination', 'Gateway', 'Metric', 'Interface', and 'Delete'. At the bottom of the screen is a 'Reset' button.

The following table describes the labels in this screen.

Table 38 Configuration > Networking > Static Route > IP Static Route

| LABEL | DESCRIPTION |
|---------------------------|--|
| Static Routing Settings | |
| Route Name | Enter a the name that describes or identifies this route. |
| Destination IP Address | Enter the IP network address of the final destination. |
| IP Subnet Netmask | This is the subnet to which the route's final destination belongs. |
| Gateway IP Address | Enter the IP address of the gateway. |
| Metric | Assign a number to identify the route. |
| Interface | Select the interface through which the traffic is routed. |
| Add Rule | Click this to add the IP static route. |
| Application Rules Summary | |
| No. | This is the number of an individual static route. |
| Active | The rules are always on and this is indicated by the icon. |
| Name | This is the name that describes or identifies this route. |
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Gateway | This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Metric | This is the number assigned to the route. |
| Interface | This is the interface through which the traffic is routed. |

Table 38 Configuration > Networking > Static Route > IP Static Route (continued)

| LABEL | DESCRIPTION |
|--------|--|
| Delete | Click the Delete icon to remove a static route from the NBG4104. A window displays asking you to confirm that you want to delete the route. |
| Reset | Click Reset to begin configuring this screen afresh. |

VLAN Operation

16.1 Overview

Use these screens to configure the VLAN ID and IEEE 802.1p priority tags for LAN to WAN and WAN to LAN traffic.

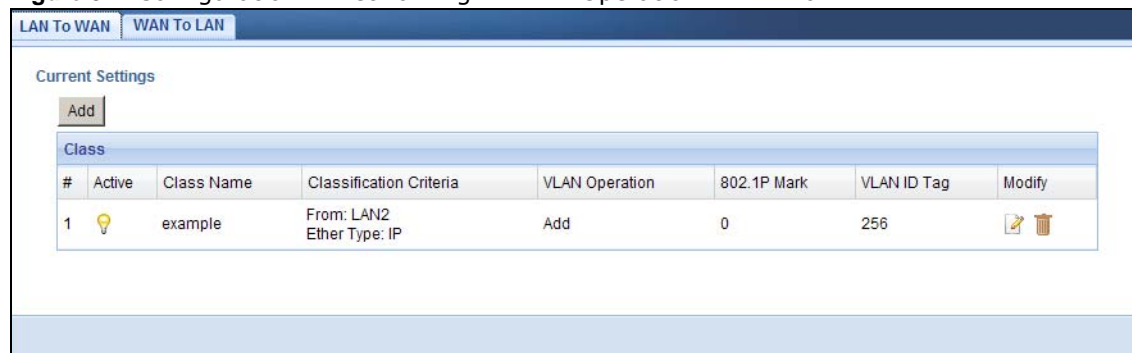
16.2 What You Can Do

- Use the **LAN To WAN** screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent from individual LAN ports ([Section 16.3 on page 101](#)).
- Use the **WAN To LAN** screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent to individual LAN ports ([Section 16.4 on page 105](#)).

16.3 LAN To WAN Screen

Click **Co figuration > Networking > VLAN Operation** to open the **LAN To WAN** screen. Use this screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent from individual LAN ports.

Figure 51 Configuration > Networking > VLAN Operation > LAN To WAN



| # | Active | Class Name | Classification Criteria | VLAN Operation | 802.1P Mark | VLAN ID Tag | Modify |
|---|--------|------------|------------------------------|----------------|-------------|-------------|--------|
| 1 | 💡 | example | From: LAN2 Ether Type: IP | Add | 0 | 256 | ✎ 🗑️ |

The following table describes the labels in this screen.

Table 39 Configuration > Networking > VLAN Operation > LAN To WAN

| LABEL | DESCRIPTION |
|------------------|--|
| Current Settings | |
| Add | Click this to create a new classifier. |
| Class | |

Table 39 Configuration > Networking > VLAN Operation > LAN To WAN (continued)

| LABEL | DESCRIPTION |
|-------------------------|--|
| # | This is the index number of the entry. |
| Active | This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active. |
| Class Name | This is the name of the classifier. |
| Classification Criteria | This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier. |
| VLAN Operation | This shows the VLAN operation used for this classifier. |
| 802.1P Mark | This is the IEEE 802.1p priority level assigned to traffic of this classifier. |
| VLAN ID Tag | This is the VLAN ID number assigned to traffic of this classifier. |
| Modify | Click the Edit icon to display and modify an existing classifier setting. Click the Remove icon to delete a classifier. |

16.3.1 Add/Edit VLAN Rule

Click **Add** in the **LAN to WAN** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 52 LAN To WAN > Add/Edit

Please fill up steps 1 through 4 to configure a VLAN rule.

Step1: Class configuration

Active

Class Name:

Classification Order:

Step2: Criteria configuration

Use the fields below to specify the characteristics of a data flow that needs to be managed by this QoS rule.

Basic

From Interface:

Ether Type:

Source

Address: subnet Mask: Exclude

Port Range: ~ Exclude

MAC: MAC Mask: Exclude

Destination

Address: subnet Mask: Exclude

Port Range: ~ Exclude

Others

IP Protocol: Exclude

DSCP: (0~63) Exclude

Step3: VLAN tag

The VLAN tag can be added, remark and remove by applying the following settings:

VLAN Operation:

802.1P Mark:

VLAN ID: (10~4094)

The following table describes the labels in this screen.

Table 40 LAN To WAN: Add/Edit

| LABEL | DESCRIPTION |
|------------------------|--|
| Class configuration | |
| Active | Select this to enable this classifier. |
| Class Name | Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces. |
| Classification Order | Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking Apply . Select Last to put this rule in the back of the classifier list. |
| Criteria configuration | |
| Basic | |

Table 40 LAN To WAN: Add/Edit (continued)

| LABEL | DESCRIPTION |
|----------------|---|
| From Interface | If you want to classify the traffic by an ingress interface, select an interface from the From Interface drop-down list box. |
| Ether Type | <p>Select a predefined application to configure a class for the matched traffic.</p> <p>If you select IP, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type.</p> <p>If you select 802.1Q, you can configure an 802.1p priority level.</p> |
| Source | |
| Address | Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| Subnet Mask | Enter the source subnet mask. |
| Port Range | If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source. |
| MAC | Select the check box and enter the source MAC address of the packet. |
| MAC Mask | <p>Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.</p> |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| Destination | |
| Address | Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| Subnet Mask | Enter the source subnet mask. |
| Port Range | If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source. |
| MAC | Select the check box and enter the source MAC address of the packet. |
| MAC Mask | <p>Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.</p> |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| Others | |
| IP Protocol | <p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select the protocol (service type) from TCP, UDP, ICMP or IGMP. If you select User defined, enter the protocol (service type) number.</p> |
| DSCP | <p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.</p> |
| VLAN tag | |

Table 40 LAN To WAN: Add/Edit (continued)

| LABEL | DESCRIPTION |
|----------------|--|
| VLAN Operation | <p>If you select Add, the NBG4104 treat all matched traffic untagged and add a second VLAN ID.</p> <p>If you select Remark VLAN ID, enter a VLAN ID number in the VLAN ID field below with which the NBG4104 replaces the VLAN ID of the frames.</p> <p>If you select Remark 1P, select a priority level from the 802.1P Mark field below with which the NBG4104 replaces the IEEE 802.1p priority field in the packets.</p> <p>If you select Remark VLAN ID and 1P, select a priority level from the 802.1P Mark field and enter a VLAN ID number in the VLAN ID field below.</p> <p>If you select Remove, the NBG4104 deletes the VLAN ID of the frames before forwarding them out.</p> |
| 802.1P Mark | <p>Select a priority level with which the NBG4104 replaces the IEEE 802.1p priority field in the packets.</p> <p>If you select Unchange, the NBG4104 keep the 802.1p priority field in the packets.</p> |
| VLAN ID | Enter a VLAN ID number with which the NBG4104 replaces the VLAN ID of the frames. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |
| Reset | Click Reset to begin configuring this screen afresh. |

16.4 WAN To LAN Screen

Click **Configuration > Networking > VLAN Operation > WAN To LAN** to open this screen. Use this screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent to individual LAN ports.

Figure 53 Configuration > Networking > VLAN Operation > WAN To LAN

The screenshot shows the 'WAN To LAN' configuration screen. At the top, there are two tabs: 'LAN To WAN' and 'WAN To LAN'. Below the tabs is the title 'LAN VLAN Setup'. The main content is a table with the following columns: 'Interface', 'Lan Port', 'TAG Operation', '802.1P Mark', and 'VLAN ID'. The table has four rows for LAN1, LAN2, LAN3, and LAN4. For each row, the 'TAG Operation' is set to 'Unchange', the '802.1P Mark' is set to '0 BE', and the 'VLAN ID' field is empty. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

| Interface | Lan Port | TAG Operation | 802.1P Mark | VLAN ID |
|-----------|----------|---------------|-------------|---------|
| | LAN1 | Unchange | 0 BE | |
| | LAN2 | Unchange | 0 BE | |
| | LAN3 | Unchange | 0 BE | |
| | LAN4 | Unchange | 0 BE | |

The following table describes the labels in this screen.

Table 41 Configuration > Networking > VLAN Operation > WAN To LAN

| LABEL | DESCRIPTION |
|---------------|--|
| Lan Port | These represent the NBG4104's LAN ports. |
| TAG Operation | <p>Select what you want the NBG4104 to do to the IEEE 802.1q VLAN ID and priority tags of downstream traffic before sending it out through this LAN port.</p> <ul style="list-style-type: none"> • Unchange - Don't do anything to the traffic's VLAN ID and priority tags. • Add - Add VLAN ID and priority tags to untagged traffic. • Remark VLAN ID - Change the value of the outer VLAN ID. • Remark 1P - Change the value of the priority tags. • Remark VLAN ID and 1P - Change the value of the outer VLAN ID and priority tags. • Remove - Delete one tag from tagged traffic. If the frame has double tags, this removes the outer tag. This does not affect untagged traffic. |
| 802.1P Mark | Use this option to set what to do for the IEEE 802.1p priority tags when you add or remark the tags for a LAN port's downstream traffic. Either select Unchange to not modify the traffic's priority tags or select an priority from 0 to 7 to use. The larger the number, the higher the priority. |
| VLAN ID | If you will add or remark tags for this LAN port's downstream traffic, specify the VLAN ID (from 0 to 4094) to use here. |
| Apply | Click Apply to save your changes. |
| Reset | Click Reset to begin configuring this screen afresh. |

Interface Group

17.1 Overview

By default, all LAN and WAN interfaces on the NBG4104 are in the same group and can communicate with each other. You can create multiple groups to have the NBG4104 assign the IP addresses in different domains to different groups. Each group acts as an independent network on the NBG4104.

17.2 The Interface Group Screen

You can manually add a LAN interface or a VLAN ID to a new group. Click **Configuration > Networking > Interface Group** to open the following screen.

Figure 54 Configuration > Networking > Interface Group

| Name | LAN Interface | VLAN | WAN Interface | Modify |
|---------|---------------|------|---------------|--------|
| Default | LAN4 | | | |
| | LAN3 | | | |
| | LAN2 | | | |
| | NBG4104 | | WAN1 | |
| | NBG4104_2 | | | |
| test1 | LAN1 | | | |
| | NBG4104_1 | 456 | br1 | |

The following table describes the fields in this screen.

Table 42 Configuration > Networking > Interface Group

| LABEL | DESCRIPTION |
|----------------|---|
| Add | Click this to add a new interface grouping rule. You must configure a WAN connection before you can add a new interface grouping rule. See Chapter 10 on page 69 for more information. |
| Name | This shows the descriptive name of the group. |
| LAN Interfaces | This shows the LAN interfaces in the group. |
| VLAN | This shows the VLAN ID configured in the group. |

Table 42 Configuration > Networking > Interface Group (continued)

| LABEL | DESCRIPTION |
|----------------|---|
| WAN Interfaces | This shows the WAN interfaces in the group. |
| Modify | Select the Delete icon to delete the group from the NBG4104. |

17.2.1 Interface Group Configuration

Click the **Add** button in the **Interface Group** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to a group only.

Figure 55 Interface Grouping Configuration

The following table describes the fields in this screen.

Table 43 Interface Grouping Configuration

| LABEL | DESCRIPTION |
|-------------------------------------|---|
| Group Name | Enter a name to identify this group. |
| WAN Interfaces used in the grouping | Select the WAN interface this group uses. The group can have up to one PTM interface and up to one ATM interface. |

Table 43 Interface Grouping Configuration (continued)

| LABEL | DESCRIPTION |
|--------------------------|--|
| Grouped LAN Interfaces | Select a LAN or WAN interface in Available LAN Interfaces and use the left-facing arrow to move it to the Grouped LAN Interfaces to add the interface to this group. |
| Available LAN Interfaces | To remove a LAN or WAN interface from the Grouped LAN Interfaces , select it and click the right-facing arrow. |
| Grouped VLAN | Enter a VLAN ID in the VLAN ID field and use the left-facing arrow to move it to the Grouped VLAN to add it to a VLAN group. To remove a VLAN ID from the Grouped VLAN , select it and click the right-facing arrow. |
| Apply | Click Apply to save your changes. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

18.1 Overview

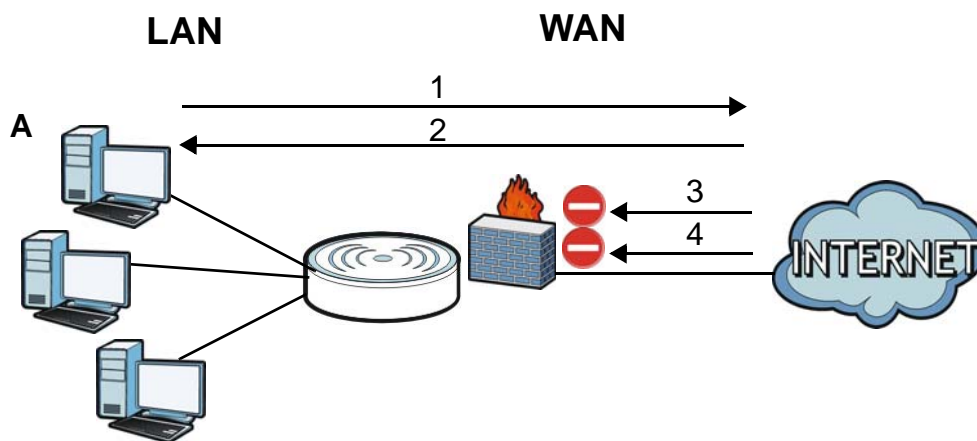
Use these screens to enable and configure the firewall that protects your NBG4104 and your LAN from unwanted or malicious traffic.

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 56 Default Firewall Action



18.2 What You Can Do

- Use the **General** screen to enable or disable the NBG4104's firewall ([Section 18.4 on page 113](#)).
- Use the **Access Control Rule** screen to view the configured access control rules and edit or remove a rule ([Section 18.5.1 on page 115](#)).
- Use the **Services** screen to configure the NBG4104's ICMP settings ([Section 18.6 on page 116](#)).

18.3 What You Need To Know

The following terms and concepts may help as you read through this chapter.

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.

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.

About the NBG4104 Firewall

The NBG4104's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is 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 NBG4104's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG4104 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 NBG4104 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 NBG4104 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, and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

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.

18.4 The Firewall General Screen

Use this screen to enable or disable the NBG4104's firewall, and set up firewall logs. Click **Configuration > Security > Firewall** to open the **General** screen.

Figure 57 Configuration > Security > Firewall > General I

The following table describes the labels in this screen.

Table 44 Configuration > Security > Firewall > General

| LABEL | DESCRIPTION |
|------------------------|--|
| Enable Firewall | Select this check box to activate the firewall. The NBG4104 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. |
| Enable Anti-DoS Attack | Select this check box to activate the Anti-Dos Attack function. |
| Apply | Click Apply to save the settings. |
| Reset | Click Reset to start configuring this screen again. |

18.5 The Access Control Rule Screen

Click **Configuration > Security > Firewall > Access Control Rule** to display the following screen. This screen displays a list of the configured access control rules.

Figure 58 Configuration > Security > Firewall > Access Control Rule

The following table describes the labels in this screen.

Table 45 Configuration > Security > Firewall > Access Control Rule

| LABEL | DESCRIPTION |
|---------------------------|--|
| Application Rules Summary | |
| Packet Direction | Select the direction of traffic (WAN to LAN or WAN to WAN) to which this rule applies. |
| Firewall Rule | |
| # | This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. |
| Name | This displays the name of the rule. |
| Source MAC | This is the source MAC address of the rule. |
| Dest IP | This column displays the destination addresses to which this firewall rule applies. |
| Source IP | This column displays the source addresses to which this firewall rule applies. |
| Protocol | This displays the IP port that defines your customized port. |
| Dest. Port Range | This column displays the port number or the range of port numbers of the destination. |
| Source Port Range | This column displays the port number or the range of port numbers of the source. |
| Action | This field displays whether the rule silently discards packets (Drop) or allows the passage of packets (Allow). |
| Delete | Click the Edit icon to display and modify an existing firewall rule setting. Click the Remove icon to delete a firewall rule. |

Table 45 Configuration > Security > Firewall > Access Control Rule (continued)

| LABEL | DESCRIPTION |
|-------|--|
| Apply | Click Apply to save the settings. |
| Reset | Click Reset to start configuring this screen again. |

18.5.1 Access Control Rule Edit

Click the **Edit** icon next to a firewall rule in the **Access Control Rule** screen. The following screen is displayed. You can use this screen to modify a rule.

Figure 59 Access Control Rule: Edit

The screenshot shows a configuration form for an Access Control Rule. The fields are as follows:

- Rule Name:
- Source MAC:
- Dest. IP:
- Source IP:
- Protocol Type:
- Dest. Port Range: - (1~65535)
- Source Port Range: - (1~65535)
- Action:

At the bottom of the form are two buttons: **Apply** and **Reset**.

The following table describes the labels in this screen.

Table 46 Access Control Rule: Edit

| LABEL | DESCRIPTION |
|-------------------|---|
| Rule Name | Enter a descriptive name for the rule. |
| Source MAC | Enter the source MAC address of the rule. |
| Dest IP | Enter the destination addresses to which this rule applies. |
| Source IP | Enter the source addresses to which this rule applies. |
| Protocol Type | Choose the IP port (TCP , UDP , or ICMP) that defines your customized port from the drop-down list box. If you do not want to configure the IP port, select None . |
| Dest. Port Range | Enter the port number or the range of port numbers of the destination. |
| Source Port Range | Enter the port number or the range of port numbers of the source. |
| Action | Select the action for the rule: <ul style="list-style-type: none"> • Drop: silently discards packets. • Allow: allows the passage of packets. |
| Apply | Click Apply to save the settings. |
| Reset | Click Reset to start configuring this screen again. |

See [Appendix F on page 227](#) for commonly used services and port numbers.

18.6 The Services Screen

If an outside user attempts to probe an unsupported port on your NBG4104, an ICMP response packet is automatically returned. This allows the outside user to know the NBG4104 exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG4104 when unsupported ports are probed.

Click **Configuration > Security > Firewall > Services** to display the following screen.

Figure 60 Configuration > Security > Firewall > Services

The following table describes the labels in this screen.

Table 47 Configuration > 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 NBG4104 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. |
| Apply | Click Apply to save the settings. |
| Reset | Click Reset to start configuring this screen again. |

Content Filtering

19.1 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.

19.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Content Filtering Profiles

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.

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

Keyword Blocking URL Checking

The NBG4104 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.

Since the NBG4104 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 NBG4104 would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

19.3 Content Filter

Use this screen to restrict web features, add keywords for blocking and designate a trusted computer. Click **Configuration > Security > Content Filter** to open the **Content Filter** screen.

Figure 61 Configuration > Security > Content Filter

The following table describes the labels in this screen.

Table 48 Configuration > Security > Content Filter

| LABEL | DESCRIPTION |
|-----------------------------|--|
| Trusted Computer IP Address | To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers. |
| Restrict Web Features | Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out. |
| ActiveX | A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. |
| Java | A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds. |
| Cookies | Used by Web servers to track usage and provide service based on ID. |
| Web Proxy | A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server. |

Table 48 Configuration > Security > Content Filter (continued)

| LABEL | DESCRIPTION |
|-----------------------------|--|
| Enable URL Keyword Blocking | The NBG4104 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. |
| 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. |
| Keyword List | This list displays the keywords already added. |
| 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. |
| Apply | Click Apply to save your changes. |
| Reset | Click Reset to begin configuring this screen afresh |

19.4 Technical Reference

The following section contains additional technical information about the NBG4104 features described in this chapter.

19.4.1 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 NBG4104 checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG4104 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 NBG4104 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 NBG4104 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.

Remote Management

20.1 Overview

This chapter provides information on the Remote Management screens.

Remote Management allows you to manage your NBG4104 from a remote location through the following interfaces:

- LAN and WAN
- LAN only

Note: The NBG4104 is managed using the Web Configurator.

20.2 What You Need to Know

Remote management over LAN or WAN will not work when:

- 1 The IP address in the **Secured Client IP Address** field ([Section 20.4 on page 122](#)) does not match the client IP address. If it does not match, the NBG4104 will disconnect the session immediately.
- 2 There is already another remote management session. You may only have one remote management session running at one time.
- 3 There is a firewall rule that blocks it.

20.2.1 Remote Management and NAT

When NAT is enabled:

- Use the NBG4104's WAN IP address when configuring from the WAN.
- Use the NBG4104's LAN IP address when configuring from the LAN.

20.3 What You Can Do

- Use the **WWW** screen to configure through which interface(s) and from which IP address(es) users can use HTTP or HTTPS to manage the NBG4104 ([Section 20.4 on page 122](#)).
- Use the **Telnet** screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG4104 ([Section 20.5 on page 123](#)).

- Use the **FTP** screen to configure through which interface(s) and from which IP address(es) users can use to access the NBG4104 ([Section 20.6 on page 124](#)).
- Your NBG4104 can act as an SNMP agent, which allows a manager station to manage and monitor the NBG4104 through the network. Use the **SNMP** screen to configure SNMP settings. You can also specify from which IP addresses the access can come ([Section 20.7 on page 124](#)).
- Use the **TR069** screen to configure the NBG4104's TR-069 auto-configuration settings ([Section 20.8 on page 127](#)).
- Use the **Import CA** screen to import CA certificates to the NBG4104 ([Section 20.9 on page 128](#)).

20.4 The WWW Screen

To change your NBG4104's remote management settings, click **Configuration > Management > Remote MGMT** to open the **WWW** screen.

Figure 62 Configuration > Management > Remote MGMT > WWW

The following table describes the labels in this screen.

Table 49 Configuration > Management > Remote MGMT > WWW

| LABEL | DESCRIPTION |
|---------------------------|---|
| HTTPS | |
| Server Port | You may change the server port number for a HTTPS 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 NBG4104 using this HTTPS service. |
| Secured Client IP Address | Select All to allow all computers to access the NBG4104. Otherwise, check Selected and specify the IP address of the computer that can access the NBG4104. |
| HTTP | |
| Server Port | You may change the server port number for a HTTP 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 NBG4104 using this HTTP service. |

Table 49 Configuration > Management > Remote MGMT > WWW (continued)

| LABEL | DESCRIPTION |
|---------------------------|---|
| Secured Client IP Address | Select All to allow all computers to access the NBG4104. Otherwise, check Selected and specify the IP address of the computer that can access the NBG4104. |
| Apply | Click Apply to save your customized settings and exit this screen. |
| Reset | Click Reset to begin configuring this screen afresh. |

20.5 The Telnet Screen

You can use Telnet to access the NBG4104's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **Configuration > Management > Remote MGMT > Telnet** to display the screen as shown.

Figure 63 Configuration > Management > Remote MGMT > Telnet

The following table describes the labels in this screen.

Table 50 Configuration > Management > Remote MGMT > Telnet

| LABEL | DESCRIPTION |
|---------------------------|---|
| TELNET | |
| 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 NBG4104 using this service. |
| Secured Client IP Address | Select All to allow all computers to access the NBG4104. Otherwise, check Selected and specify the IP address of the computer that can access the NBG4104. |
| Apply | Click Apply to save your customized settings and exit this screen. |
| Reset | Click Reset to begin configuring this screen afresh. |

20.6 The FTP Screen

Use this screen to specify which interfaces allow access and from which IP address the access can come. To change your NBG4604's settings, click **Configuration > Management > Remote MGMT >** to display the screen as shown.

Figure 64 Configuration > Management > Remote MGMT > FTP

The following table describes the labels in this screen.

Table 51 Configuration > Management > Remote MGMT > FTP

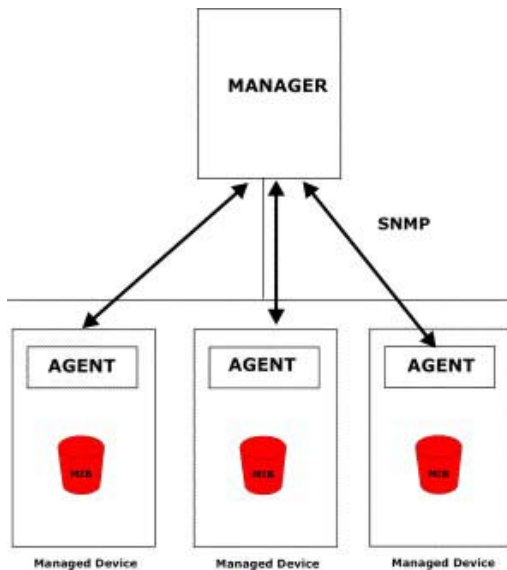
| LABEL | DESCRIPTION |
|---------------------------|---|
| Server Port | You may change the server port number for a service if needed. However you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the NBG4104 using this service. |
| Secured Client IP Address | Select All to allow all computers to access the NBG4104. Otherwise, check Selected and specify the IP address of the computer that can access the NBG4104. |
| Apply | Click Apply to save your customized settings and exit this screen. |
| Reset | Click Reset to begin configuring this screen afresh. |

20.7 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your NBG4104 supports SNMP agent functionality, which allows a manager station to manage and monitor the NBG4104 through the network. The NBG4104

supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 65 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the NBG4104). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

To change your NBG4104's SNMP settings, click **Configuration > Management > Remote MGMT > SNMP** to display the screen as shown.

Figure 66 Configuration > Management > Remote MGMT > SNMP

The following table describes the labels in this screen.

Table 52 Configuration > Management > Remote MGMT > SNMP

| LABEL | DESCRIPTION |
|---------------------------|---|
| SNMP Settings | |
| Server Port | The SNMP agent listens on port 161 by default. If you change the SNMP server port to a different number on the NBG4104, for example 8161, then you must notify people who need to access the NBG4104 SNMP agent to use the same port. |
| Server Access | Select the interface(s) through which a computer may access the NBG4104 using this service. |
| Secured Client IP Address | Select All to allow all computers to access the NBG4104. Otherwise, check Selected and specify the IP address of the computer that can access the NBG4104. |
| SNMP Settings | |
| Enable SNMP | Select this to enable SNMP on this device. |
| Get Community | Enter the SNMP get community information here. |
| Set Community | Enter the SNMP set community information here. |
| System Location | Enter the SNMP system location. |
| System Contact | Enter the SNMP system contact. |
| Trap Settings | |
| Trap Settings | Select this to enable trap settings on this device. |
| Trap Manager IP | Type the IP address of the station to send your SNMP traps to. |
| Trap Community | Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. |

Table 52 Configuration > Management > Remote MGMT > SNMP (continued)

| LABEL | DESCRIPTION |
|-------|---|
| Apply | Click Apply to save your customized settings and exit this screen. |
| Reset | Click Reset to begin configuring this screen afresh. |

20.8 The TR069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your ZyXEL Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the NBG4104, modify settings, perform firmware upgrades as well as monitor and diagnose the NBG4104. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Configuration > Management > Remote MGMT > TR069** to display the screen as shown. Use this screen to configure your NBG4104 to be managed by an ACS.

Figure 67 Configuration > Management > Remote MGMT > TR069

The following table describes the labels in this screen.

Table 53 Configuration > Management > Remote MGMT > TR069

| LABEL | DESCRIPTION |
|-----------------|--|
| TR069 Client | |
| Inform | Select Enable for the NBG4104 to send periodic inform via TR-069 on the WAN. Otherwise, select Disable . |
| Inform Interval | Enter the time interval (in seconds) at which the NBG4104 sends information to the auto-configuration server. |
| ACS URL | Enter the URL or IP address of the auto-configuration server. |
| ACS Username | Enter the TR-069 user name for authentication with the auto-configuration server. |
| ACS Password | Enter the TR-069 password for authentication with the auto-configuration server. |

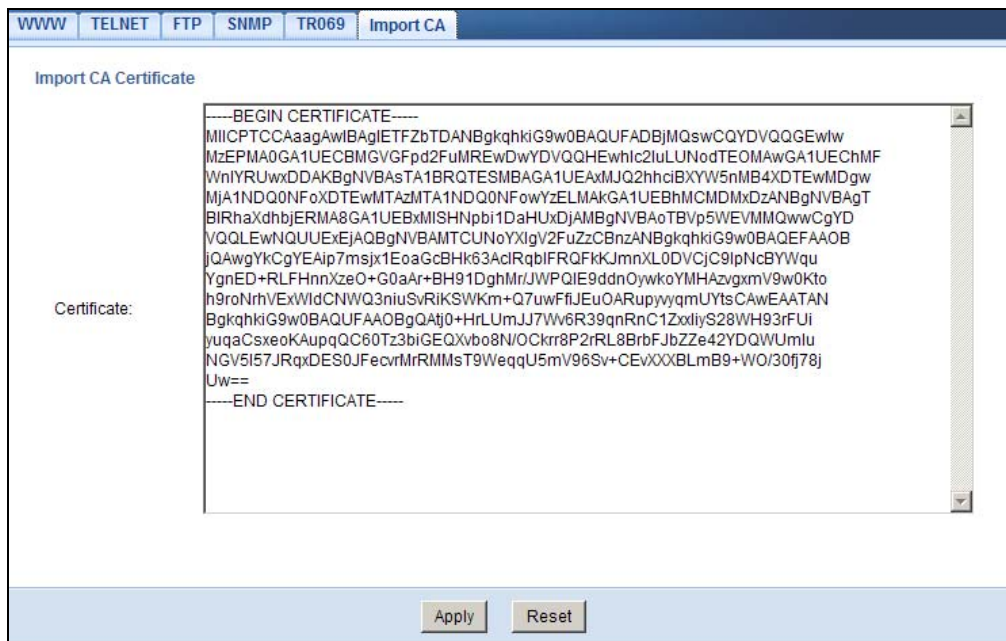
Table 53 Configuration > Management > Remote MGMT > TR069 (continued)

| LABEL | DESCRIPTION |
|-----------------------------|--|
| Connection Request Username | Enter the connection request user name. When the ACS makes a connection request to the NBG4104, this user name is used to authenticate the ACS. |
| Connection Request Password | Enter the connection request password. When the ACS makes a connection request to the NBG4104, this password is used to authenticate the ACS. |
| Apply | Click Apply to save your customized settings and exit this screen. |
| Reset | Click Reset to begin configuring this screen afresh. |

20.9 The Import CA Screen

The NBG4104 can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Click **Configuration > Management > Remote MGMT > Import CA** to open the following. You can view or import a certificate in this screen.

Figure 68 Configuration > Management > Remote MGMT > Import CA

The following table describes the labels in this screen.

Table 54 Configuration > Management > Remote MGMT > Import CA

| LABEL | DESCRIPTION |
|-----------------------|--|
| Import CA Certificate | You can view the details of a certificate that is already imported. If you want to change it, you can delete the old certificate and copy the new certificate of a certification authority that you trust and paste it in the space between BEGIN CERTIFICATE and END CERTIFICATE . |
| Apply | Click Apply to save your customized settings and exit this screen. |
| Reset | Click Reset to begin configuring this screen afresh. |

Bandwidth Management

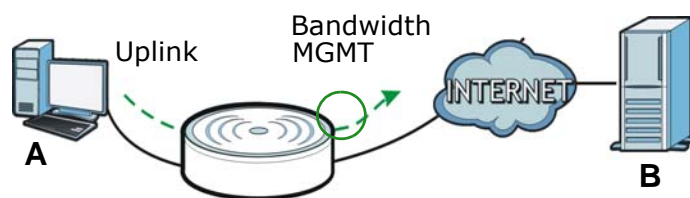
21.1 Overview

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

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

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

Figure 69 Bandwidth Management



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

21.2 What You Can Do

- Use the **General** screen to enable bandwidth management and assign uplink limits ([Section 21.4 on page 131](#)).
- Use the **Advanced** screen to configure bandwidth management rules for the pre-defined services and applications ([Section 21.5 on page 132](#)).

21.3 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Bandwidth Limiting

You can limit an application's uplink bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. Use the following guidelines:

- The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the **Uplink** value that you configure in the **Bandwidth Management General** screen.

21.4 The Bandwidth MGMT General Screen

Use this screen to enable bandwidth management and assign uplink limits. You can use either one of the following types:

- **Priority Queue.** Enable bandwidth management to give uplink traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. (This type does not apply to downlink traffic.)
- **Bandwidth Allocation.** 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.

Note: You cannot apply both bandwidth management types at the same time.

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

Figure 70 Configuration > Management > Bandwidth MGMT > General

The screenshot shows the 'General' tab of the Bandwidth MGMT configuration screen. It features a 'Service Management' section with a 'Bandwidth Management Type' dropdown menu currently set to 'Disable'. Below this is a 'Total Bandwidth' section with an 'Upstream Bandwidth' input field and a '(kbps)' label. At the bottom of the form are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 55 Configuration > Management > Bandwidth MGMT > General

| LABEL | DESCRIPTION |
|---------------------------|--|
| Service Management | |
| Bandwidth Management Type | <p>This field allows you to have NBG4104 apply bandwidth management.</p> <p>Select Disable if you do not want to use this feature.</p> <p>Select Priority Queue to allocate bandwidth based on the pre-defined priority assigned to an application. Refer to Section 21.5 on page 132.</p> <p>Select Bandwidth Allocation allocate specific amounts of bandwidth to specific protocols on an IP or IP range. Refer to Section 21.5 on page 132.</p> |
| Total Bandwidth | |
| Upstream | Select the total amount of bandwidth (from 32kbps to 100mbps) that you want to dedicate to upstream traffic. |
| Apply | Click Apply to save your customized settings. |
| Reset | Click Reset to begin configuring this screen afresh. |

21.5 The Bandwidth MGMT Advanced Screen

Use this screen to configure bandwidth managements rule for specific protocols on an IP or IP range.

Note: This screen contains the **Priority Queue** and **Bandwidth Allocation** tables. Though both tables are described in this section, you can only apply the rules in one table. Fill out the table of the **Bandwidth Management Type** you selected in the Bandwidth MGMT **General** screen.

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

Figure 71 Configuration > Management > Bandwidth MGMT > Advanced

The screenshot shows the 'Advanced' configuration screen for Bandwidth Management. It features two main sections: 'Priority Queue' and 'Bandwidth Allocation'. The 'Priority Queue' section contains a table with 8 rows, each representing a rule. Each row has columns for '#', 'Enable' (with a yellow or gray bulb icon), 'Service Name' (text input), 'Priority' (dropdown menu), and 'Specific Port' (dropdown menu and two text input fields). The 'Bandwidth Allocation' section contains a table with 8 rows, each representing a rule. Each row has columns for '#', 'Enable' (with a yellow or gray bulb icon), 'LAN IP Range' (text input), 'Port Range' (text input), 'Rate Limit' (text input), and 'Modify' (with edit and delete icons). At the bottom of the screen are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 56 Configuration > Management > Bandwidth MGMT > Advanced

| LABEL | DESCRIPTION |
|----------------|---|
| Priority Queue | |
| # | This is the number of an individual bandwidth management rule. |
| Enable | A yellow bulb indicates this rule is active. A gray bulb indicates it is disabled. |
| Service Name | Enter the name of the service. You can also enter the name (up to 10 keyboard characters) of a service you want to add in the priority queue (for example, Messenger). |
| Priority | Select a priority from the drop down list box. Choose from 1 to 4 (1 is the highest). |

Table 56 Configuration > Management > Bandwidth MGMT > Advanced (continued)

| LABEL | DESCRIPTION |
|----------------------|---|
| Specific Port | Select the port/s assigned to the service. You can also specify the port/s to services to which you want to allocate bandwidth. Choose either TCP&UDP , TCP or UDP in the drop-down menu and enter the port or range of ports in the provided boxes. Note: If you are entering a specific port and not a range of ports, you can either leave the second port field blank or enter the same port number again. |
| Bandwidth Allocation | Use this table to allocate specific amounts of bandwidth to specific protocols on an IP or IP range. |
| # | This is the number of an individual bandwidth management rule. |
| Enable | A yellow bulb indicates this rule is active. A gray bulb indicates it is disabled. |
| LAN IP Range | This displays the range of IP addresses for which the bandwidth management rule applies. |
| Port Range | This displays the range of ports for which the bandwidth management rule applies. |
| Rate Limit | This is the maximum or minimum bandwidth allowed (refer to the field above) for the rule in bits per second. |
| Modify | Click the Edit icon to open the Bandwidth Allocation Edit screen. Modify an existing rule or create a new rule in this screen. See Section 21.5.1 on page 134 for more information. Click the Delete icon to delete a rule. |
| Apply | Click Apply to save your customized settings. |
| Reset | Click Reset to begin configuring this screen afresh. |

21.5.1 User Defined Service Rule Configuration

If you want to edit a bandwidth management rule for specific protocols on an IP or IP range, click the **Edit** icon in the **Bandwidth Allocation** table of the **Advanced** screen. The following screen displays.

Figure 72 Advanced: Bandwidth Allocation Edit

Bandwidth Allocation Setup

Active

LAN IP Range: 0.0.0.0 ~ 0.0.0.0

Protocol: TCP&UDP

Port Range: ~

Max Rate: Kbps User Defined

Apply Reset Cancel

The following table describes the labels in this screen.

Table 57 Advanced: Bandwidth Allocation Edit

| LABEL | DESCRIPTION |
|--------------|--|
| Active | Select this check box to turn on this bandwidth management rule. |
| LAN IP Range | Specify the range of IP addresses for which the bandwidth management rule applies. |
| Protocol | Select the protocol (TCP&UDP , TCP , or UDP) for which the bandwidth management rule applies. |

Table 57 Advanced: Bandwidth Allocation Edit (continued)

| LABEL | DESCRIPTION |
|----------------|---|
| Port Range | Enter the range of ports for which the bandwidth management rule applies. |
| Max Rate (bps) | Select the maximum bandwidth allowed for the rule in bits per second from the drop-list. Otherwise, select User Defined and enter the rate manually. |
| Apply | Click Apply to save your customized settings. |
| Reset | Click Reset to reload the previous configuration for this screen. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

21.5.2 Services and Port Numbers

See [Appendix F on page 227](#) for commonly used services and port numbers.

Universal Plug-and-Play (UPnP)

22.1 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.

22.2 What You Need to Know

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

22.2.1 NAT Traversal

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

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

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

See the NAT chapter for more information on NAT.

22.2.2 Cautions with UPnP

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

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NBG4104 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.

22.3 UPnP Screen

Use this screen to enable UPnP on your NBG4104.

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

Figure 73 Configuration > Management > UPnP

The following table describes the fields in this screen.

Table 58 Configuration > Management > UPnP

| LABEL | DESCRIPTION |
|---|--|
| Enable the Universal Plug and Play (UPnP) Feature | Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the NBG4104's IP address (although you must still enter the password to access the web configurator). |
| Apply | Click Apply to save the setting to the NBG4104. |
| Reset | Click Reset to return to the previously saved settings. |

22.4 Technical Reference

The sections show examples of using UPnP.

22.4.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the NBG4104.

Make sure the computer is connected to a LAN port of the NBG4104. Turn on your computer and the NBG4104.

22.4.1.1 Auto-discover Your UPnP-enabled Network Device

- 1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

- 2 Right-click the icon and select **Properties**.

Figure 74 Network Connections



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

Figure 75 Internet Connection Properties



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

Figure 76 Internet Connection Properties: Advanced Settings

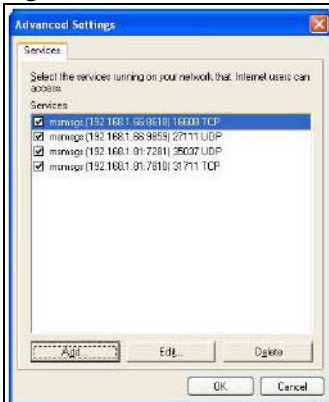
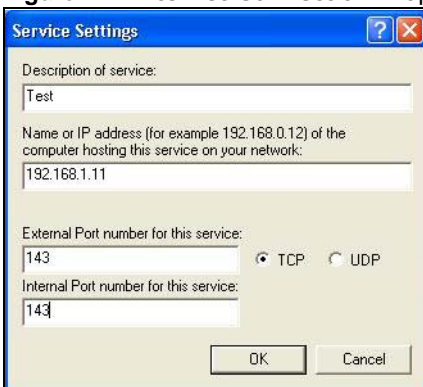


Figure 77 Internet Connection Properties: Advanced Settings: Add



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

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

Figure 78 System Tray Icon



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

Figure 79 Internet Connection Status



22.4.2 Web Configurator Easy Access

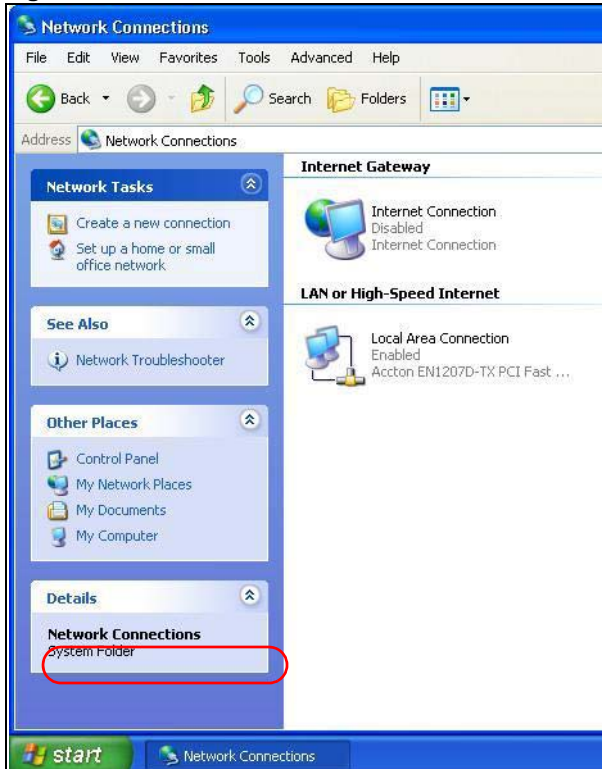
With UPnP, you can access the web-based configurator on the NBG4104 without finding out the IP address of the NBG4104 first. This comes helpful if you do not know the IP address of the NBG4104.

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**.

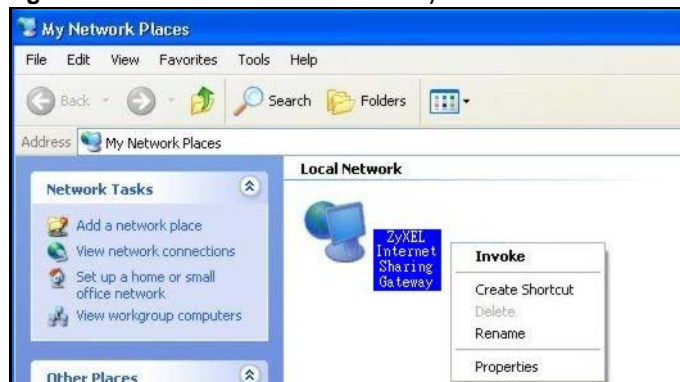
Figure 80 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your NBG4104 and select **Invoke**. The web configurator login screen displays.

Figure 81 Network Connections: My Network Places



- 6 Right-click on the icon for your NBG4104 and select **Properties**. A properties window displays with basic information about the NBG4104.

Figure 82 Network Connections: My Network Places: Properties: Example



Maintenance

23.1 Overview

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

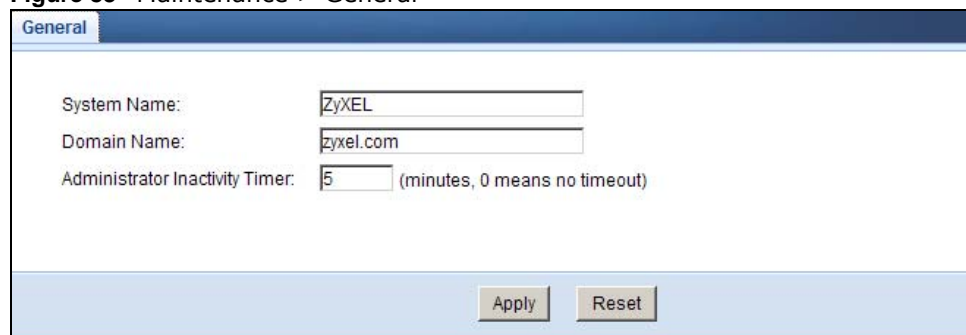
23.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session ([Section 23.3 on page 143](#)).
- Use the **Password** screen to change your NBG4104's system password ([Section 23.4 on page 144](#)).
- Use the **Time** screen to change your NBG4104's time and date ([Section 23.5 on page 145](#)).
- Use the **Firmware Upgrade** screen to upload firmware to your NBG4104 ([Section 23.6 on page 146](#)).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration ([Section 23.8 on page 148](#)).
- Use the **Restart** screen to reboot the NBG4104 without turning the power off ([Section 23.8 on page 148](#)).
- Use the **Sys OP Mode** screen to select how you want to use your NBG4104 ([Section 23.10 on page 150](#)).

23.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance > General**. The following screen displays.

Figure 83 Maintenance > General



The screenshot shows the 'General' configuration screen. It has a title bar with 'General' on the left. Below the title bar, there are three rows of configuration fields:

- System Name:** A text input field containing 'ZyXEL'.
- Domain Name:** A text input field containing 'zyxel.com'.
- Administrator Inactivity Timer:** A numeric input field containing '5', followed by the text '(minutes, 0 means no timeout)'.

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

The following table describes the labels in this screen.

Table 59 Maintenance > General

| LABEL | DESCRIPTION |
|--------------------------------|---|
| System Name | System Name is a unique name to identify the NBG4104 in an Ethernet network. |
| Domain Name | Enter the domain name you want to give to the NBG4104. |
| Administrator Inactivity Timer | Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

23.4 Password Screen

It is strongly recommended that you change your NBG4104's password.

If you forget your NBG4104's password (or IP address), you will need to reset the device. See [Section 23.8 on page 148](#) for details.

Click **Maintenance > Password**. The screen appears as shown.

Figure 84 Maintenance > Password

The following table describes the labels in this screen.

Table 60 Maintenance > Password

| LABEL | DESCRIPTION |
|-------------------|---|
| Old Password | Type the default password or the existing password you use to access the system in this field. |
| New Password | Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type. |
| Retype to Confirm | Type the new password again in this field. |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

23.5 Time Setting Screen

Use this screen to configure the NBG4104's time based on your local time zone. To change your NBG4104's time and date, click **Maintenance > Time**. The screen appears as shown.

Figure 85 Maintenance > Time

The following table describes the labels in this screen.

Table 61 Maintenance > Time

| LABEL | DESCRIPTION |
|--------------------------|---|
| Current Time and Date | |
| Current Time | This field displays the time of your NBG4104. Each time you reload this page, the NBG4104 synchronizes the time with the time server. |
| Current Date | This field displays the date of your NBG4104. Each time you reload this page, the NBG4104 synchronizes the date with the time server. |
| Current Time and Date | |
| Manual | Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it. |
| New Time (hh:mm:ss) | This field displays the last updated time from the time server or the last time configured manually. When you select 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 select Manual , enter the new date in this field and then click Apply . |
| Get from Time Server | Select this radio button to have the NBG4104 get the time and date from the time server you specified below. |

Table 61 Maintenance > Time (continued)

| LABEL | DESCRIPTION |
|----------------------------------|---|
| Auto | Select Auto to have the NBG4104 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). |
| Apply | Click Apply to save your changes back to the NBG4104. |
| Reset | Click Reset to begin configuring this screen afresh. |

23.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "NBG4104.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your NBG4104.

Figure 86 Maintenance > Firmware Upgrade

The following table describes the labels in this screen.

Table 62 Maintenance > Firmware Upgrade

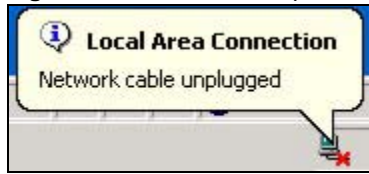
| LABEL | DESCRIPTION |
|-----------|--|
| File Path | Type in the location of the file you want to upload in this field or click Browse... to find it. |
| Browse... | Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload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

Note: Do not turn off the NBG4104 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG4104 again.

The NBG4104 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 87 Network Temporarily Disconnected



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

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

23.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the NBG4104's current configuration to a file on your computer. Once your NBG4104 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG4104.

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

Figure 88 Maintenance > Backup/Restore

Backup/Restore

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

Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path:

Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

The following table describes the labels in this screen.

Table 63 Maintenance > Backup/Restore

| LABEL | DESCRIPTION |
|-----------|---|
| Backup | Click Backup to save the NBG4104's current configuration to your computer. |
| 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 NBG4104 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 NBG4104 again. The NBG4104 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen. |
| Reset | Pressing the Reset button in this section clears all user-entered configuration information and returns the NBG4104 to its factory defaults. You can also press the RESET button on the rear panel to reset the factory defaults of your NBG4104. Refer to the chapter about introducing the Web Configurator for more information on the RESET button. |

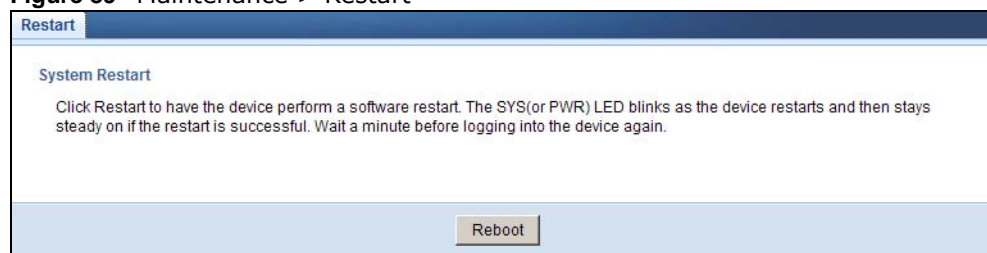
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG4104 IP address (192.168.1.2). See [Appendix D on page 185](#) for details on how to set up your computer's IP address.

23.8 Restart Screen

System restart allows you to reboot the NBG4104 without turning the power off.

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

Figure 89 Maintenance > Restart



Click **Restart** to have the NBG4104 reboot. This does not affect the NBG4104's configuration.

23.9 System Operation Mode

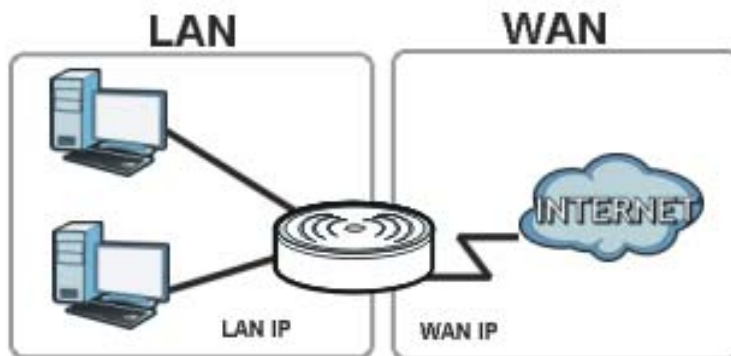
The **Sys OP Mode** (System Operation Mode) function lets you configure your NBG4104 as an router or access point. You can choose between **Router** and **Access Point Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your NBG4104.

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.

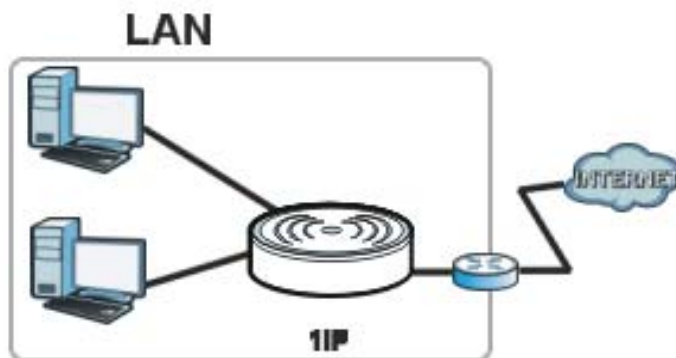
Figure 90 LAN and WAN IP Addresses in Router Mode



Access Point

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

Figure 91 Access Point Mode



23.10 Sys OP Mode Screen

Use this screen to select how you want to use your NBG4104.

Figure 92 Maintenance > Sys OP Mode

The following table describes the labels in the **Sys OP Mode** screen.

Table 64 Maintenance > Sys OP Mode

| LABEL | DESCRIPTION |
|-----------------------|--|
| System Operation Mode | |
| Router Mode | Select Router Mode if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management. You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings. |
| Access Point | Select Access Point Mode if your device bridges traffic between clients on the same network. <ul style="list-style-type: none"> In Access Point 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. The IP address of the device on the local network is set to 192.168.1.2. |
| 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 may not be able to connect to the Internet.

Troubleshooting

24.1 Overview

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](#)
- [NBG4104 Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG4104 to Its Factory Defaults](#)
- [Wireless Router/AP Troubleshooting](#)

24.2 Power, Hardware Connections, and LEDs

The NBG4104 does not turn on. None of the LEDs turn on.

- 1 Make sure you are using the power adaptor or cord included with the NBG4104.
- 2 Make sure the power adaptor or cord is connected to the NBG4104 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 NBG4104.
- 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 18](#).
- 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 NBG4104.
- 5 If the problem continues, contact the vendor.

24.3 NBG4104 Access and Login

I don't know the IP address of my NBG4104.

- 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 NBG4104 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 NBG4104 (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 NBG4104'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 NBG4104 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 NBG4104 to change all settings back to their default. This means your current settings are lost. See [Section 24.5 on page 155](#) in the **Troubleshooting** for information on resetting your NBG4104.

I forgot the username and password.

- 1 The default username is **admin** and password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 24.5 on page 155](#).

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 11.4 on page 83](#)), 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 NBG4104](#).

- 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 JavaScript and Java enabled. See [Appendix B on page 163](#).
- 4 Make sure your computer is in the same subnet as the NBG4104. (If you know that there are routers between your computer and the NBG4104, skip this step.)
 - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 11.4 on page 83](#).
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG4104. See [Section 11.4 on page 83](#).
- 5 Reset the device to its factory defaults, and try to access the NBG4104 with the default IP address. See [Section 3.3.1 on page 23](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG4104 using another service, such as Telnet. If you can access the NBG4104, check the remote management settings and firewall rules to find out why the NBG4104 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 NBG4104.

- 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 NBG4104. Log out of the NBG4104 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 NBG4104.
- 5 If this does not work, you have to reset the device to its factory defaults. See [Section 24.5 on page 155](#).

24.4 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 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.
- 3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 4 Go to **Maintenance > Sys OP Mode**. Check your **Configuration Mode** setting.
 - Select **Router Mode** 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.
- 5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG4104), 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 18](#).
- 2 Reboot the NBG4104.
- 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 18](#). If the NBG4104 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 NBG4104 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 NBG4104.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

24.5 Resetting the NBG4104 to Its Factory Defaults

If you reset the NBG4104, you lose all of the changes you have made. The NBG4104 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 NBG4104:

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the NBG4104.
- 3 Press the **RESET** button for longer than five seconds to set the NBG4104 back to its factory-default configurations.

If the NBG4104 restarts automatically, wait for the NBG4104 to finish restarting, and log in to the Web Configurator. The password is **1234**.

If the NBG4104 does not restart automatically, disconnect and reconnect the NBG4104's power. Then, follow the directions above again.

24.6 Wireless Router/AP Troubleshooting

I cannot access the NBG4104 or ping any computer from the WLAN (wireless AP or router).

- 1 Make sure the wireless LAN is enabled on the NBG4104.
- 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 NBG4104.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG4104.
- 5 Check that both the NBG4104 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 NBG4104.
- 7 Make sure you allow the NBG4104 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.

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 Filtering](#) chapter.

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

Make sure your account has access rights to the folder you are trying to open.

I cannot 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 185](#) for instructions on how to change your computer's IP address.

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

- Position the antenna for best reception. If the AP is placed on a table or floor, point the antenna upwards. If the AP is placed at a high position, point the antenna downwards. Try pointing the antenna in different directions and check which provides the strongest signal to the wireless clients.

Product Specifications

The following tables summarize the NBG4104's hardware and firmware features.

Table 65 Hardware Features

| | |
|-----------------------|--|
| Dimensions | 162 mm (W) x 115 mm (D) x 33 mm (H) |
| Weight | 205g (0.45 lb.) |
| SDRAM | 32 MB |
| Flash Memory | 8 MB |
| Power Specification | Input: 100~240 AC, 50~60 Hz Output: 12 V DC 0.5A |
| 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. |
| Built-in Switch | The NBG4104 can support speeds from 10 Mbps to 100 Mbps and you can connect multiple computers or servers (for example, game servers) in your network to the NBG4104. |
| LEDs | Power, WPS, WAN, WLAN, LAN1-4 |
| Reset button | The reset button is built into the rear panel. Use this button to restore the NBG4104 to its factory default settings. Press for longer than 1 second to restart the device. Press for more than 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 NBG4104 is equipped with one 2dBi (2.4GHz) detachable antenna to provide clear radio transmission and reception on the wireless network. |
| Operation Environment | Temperature: 0° C ~ 40° C Humidity: 20% ~ 85% Non-Condensing |
| Storage Environment | Temperature: -20° C ~ 60° C Humidity: 20% ~ 90% Non-Condensing |

Table 66 Firmware Features

| FEATURE | DESCRIPTION |
|-------------------------|---|
| Default LAN IP Address | 192.168.1.1 (router) 192.168.1.2. (AP) |
| Default LAN Subnet Mask | 255.255.255.0 (24 bits) |
| Default User Name | admin |
| Default Password | 1234 |
| DHCP Pool | 192.168.1.33 to 192.168.1.64 |
| Wireless Interface | Wireless LAN |
| Default Wireless SSID | ZyXEL |

Table 66 Firmware Features (continued)

| FEATURE | DESCRIPTION |
|--|---|
| Device Management | Use the Web Configurator to easily configure the rich range of features on the NBG4104. |
| Wireless Functionality | Allows IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the NBG4104 wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The NBG4104 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 NBG4104. Note: Only upload firmware for your specific model! |
| Configuration Backup & Restoration | Make a copy of the NBG4104's configuration and put it back on the NBG4104 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 NBG4104 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. |
| Content Filter | The NBG4104 blocks web sites with URLs that contain keywords that you specify. |
| 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 traffic for example) from a computer on a network (LAN or WAN for example) can access the NBG4104. |
| 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 NBG4104. 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 NBG4104 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 NBG4104 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. |
| Universal Plug and Play (UPnP) | The NBG4104 can communicate with other UPnP enabled devices in a network. |

24.7 Wall-mounting Instructions

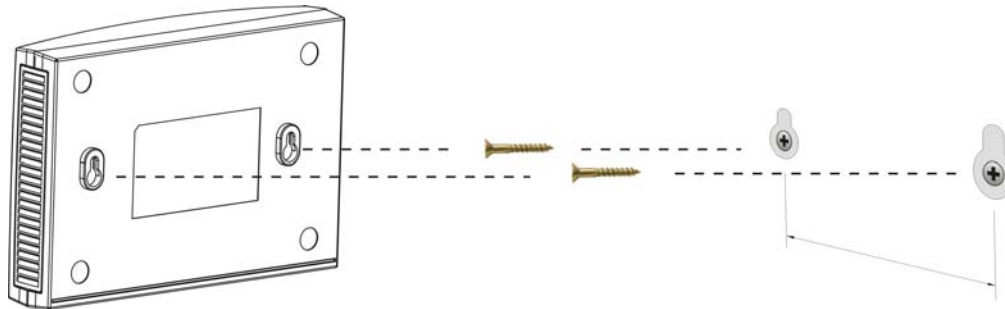
Complete the following steps to hang your NBG4104 on a wall.

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

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

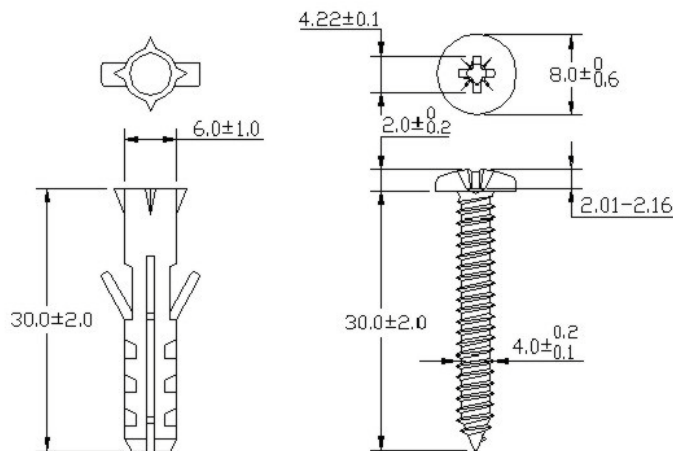
- 3 Do not insert the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the NBG4104 with the connection cables.
- 5 Align the holes on the back of the NBG4104 with the screws on the wall. Hang the NBG4104 on the screws.

Figure 93 Wall-mounting Example



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

Figure 94 Masonry Plug and M4 Tap Screw



Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

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

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

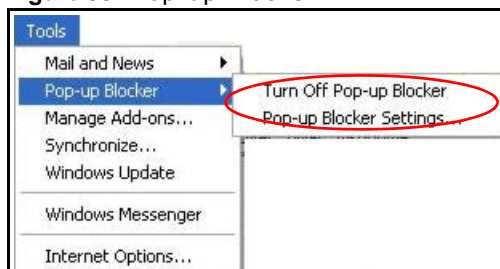
You may have to disable pop-up blocking to log into your device.

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 95 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 96 Internet Options: Privacy



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

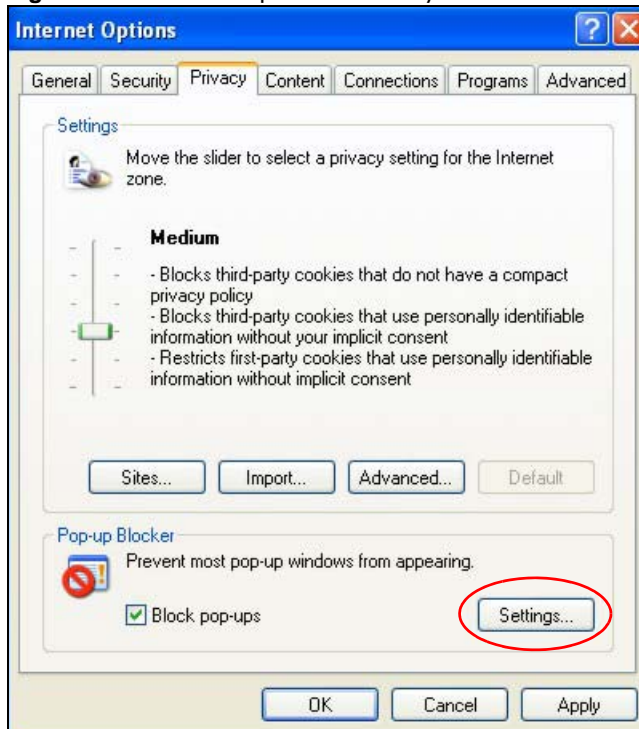
Enable Pop-up Blockers with Exceptions

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.

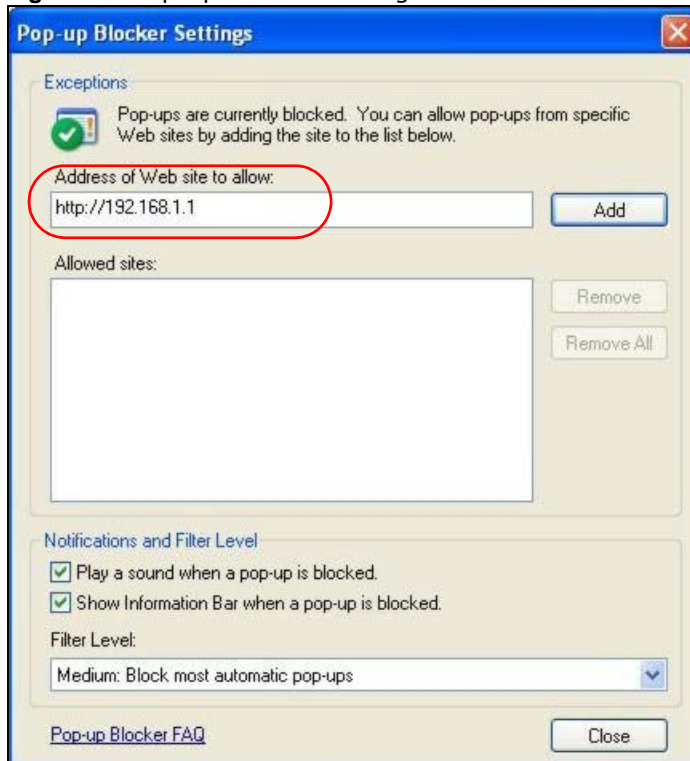
Figure 97 Internet Options: Privacy



- 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 98 Pop-up Blocker Settings



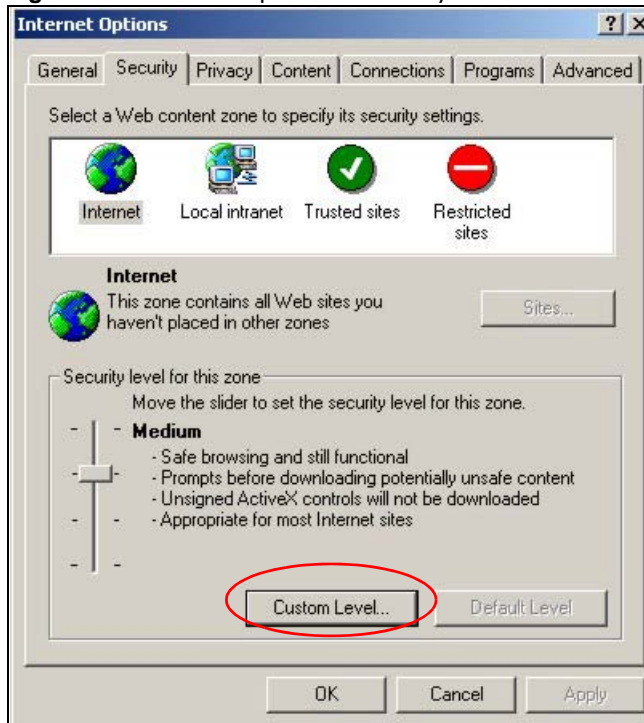
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

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

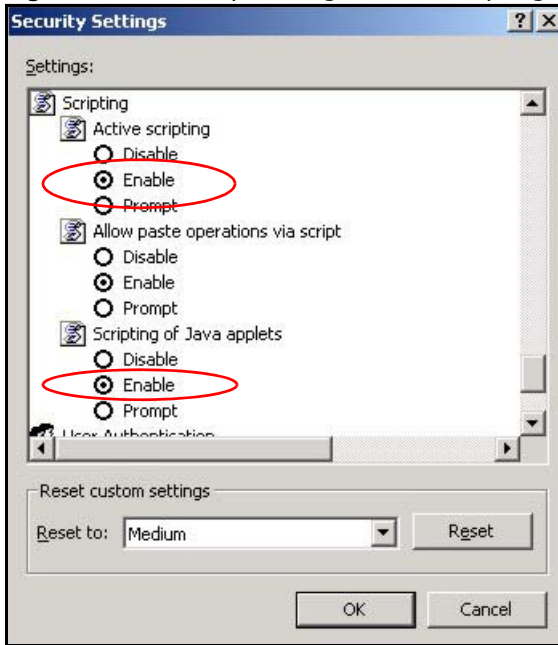
Figure 99 Internet Options: Security



- 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 100 Security Settings - Java Scripting

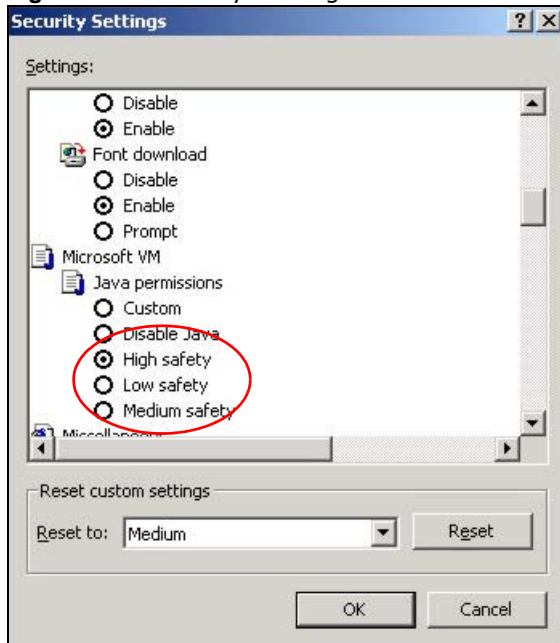


Java Permissions

- 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 101 Security Settings - Java

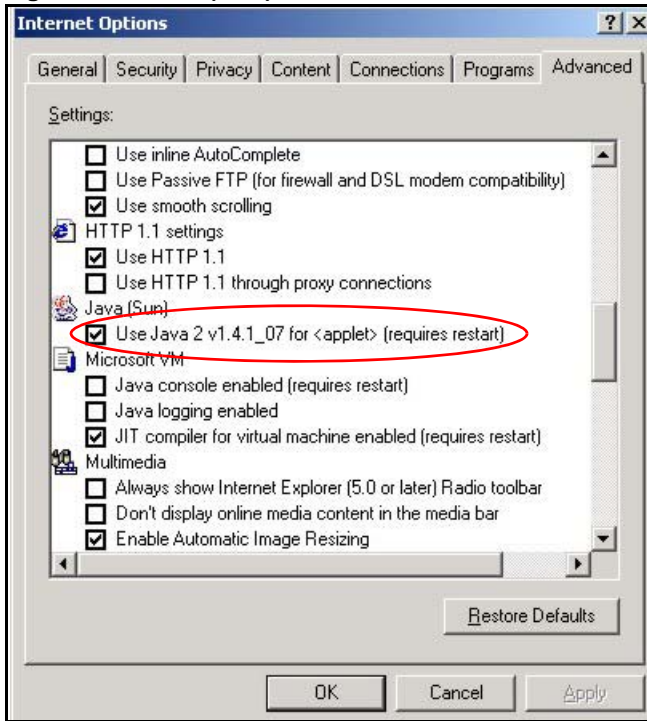


JAVA (Sun)

- 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 102 Java (Sun)

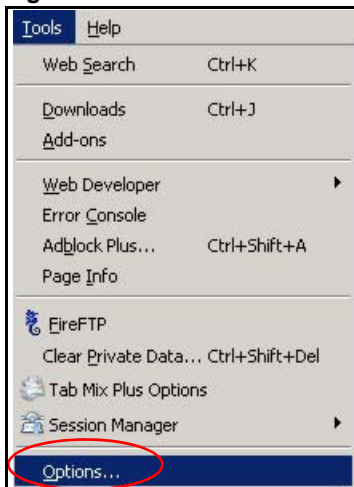


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

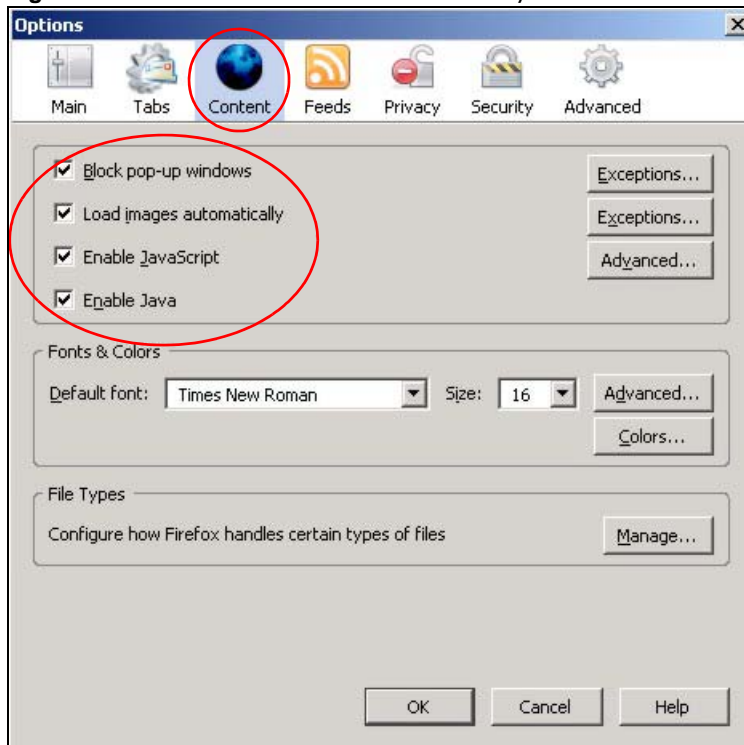
You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 103 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 104 Mozilla Firefox Content Security



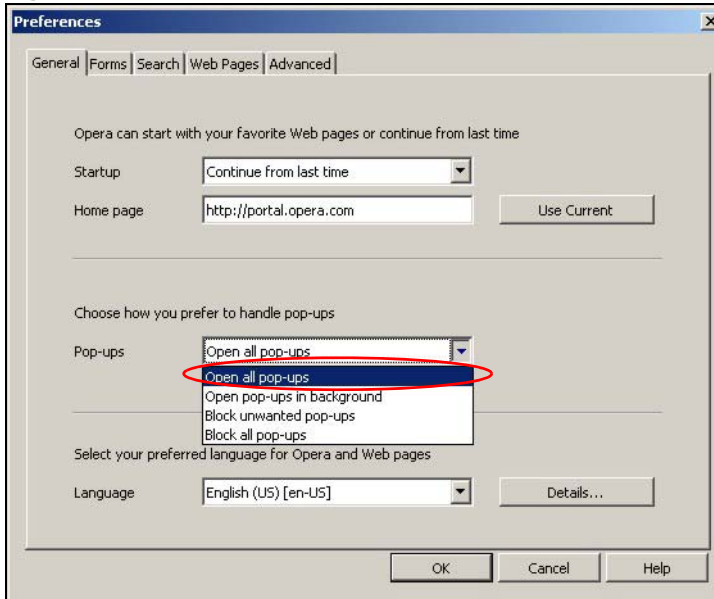
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

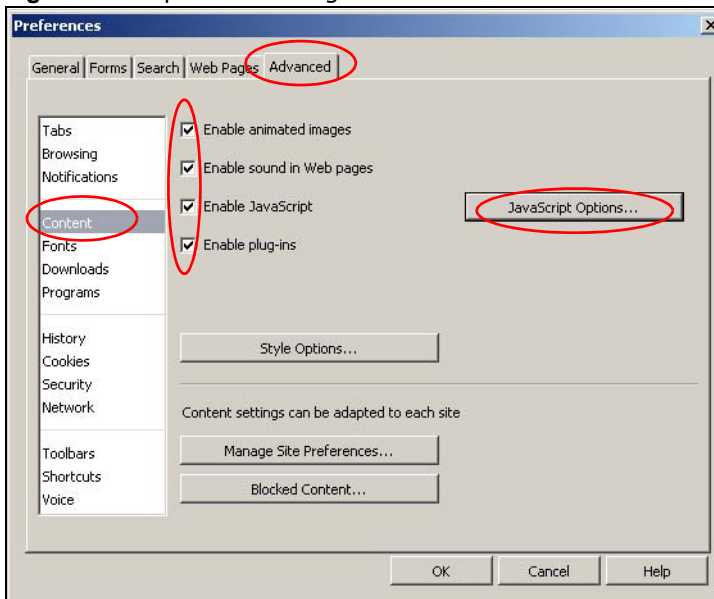
Figure 105 Opera: Allowing Pop-Ups



Enabling Java

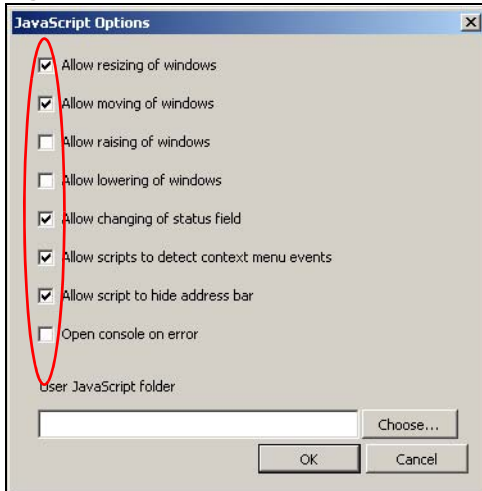
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 106 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 107 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

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.

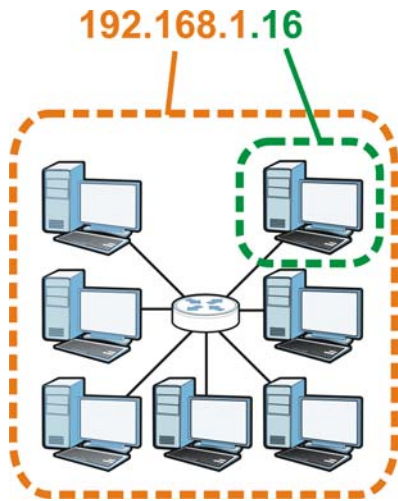
Structure

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 108 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 IP Address Network Number and Host ID Example

| | 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 |
| 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 |

Table 70 Alternative Subnet Mask Notation (continued)

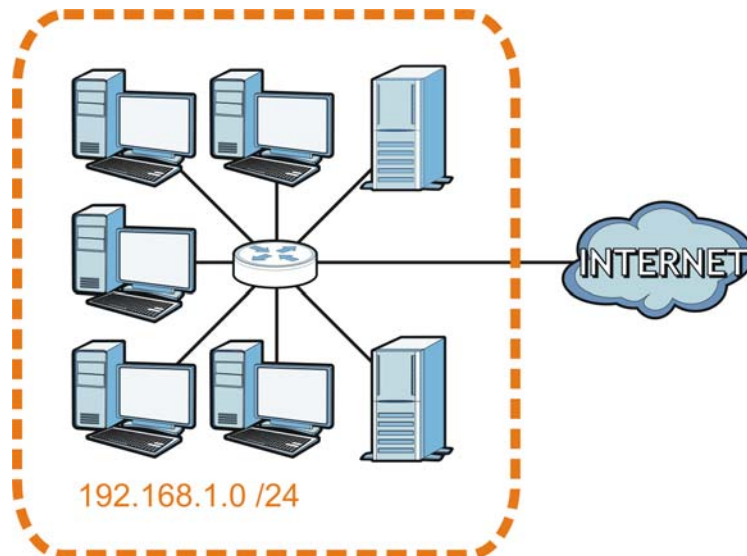
| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|-----------------|----------------------|---------------------|----------------------|
| 255.255.255.224 | /27 | 1110 0000 | 224 |
| 255.255.255.240 | /28 | 1111 0000 | 240 |
| 255.255.255.248 | /29 | 1111 1000 | 248 |
| 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.

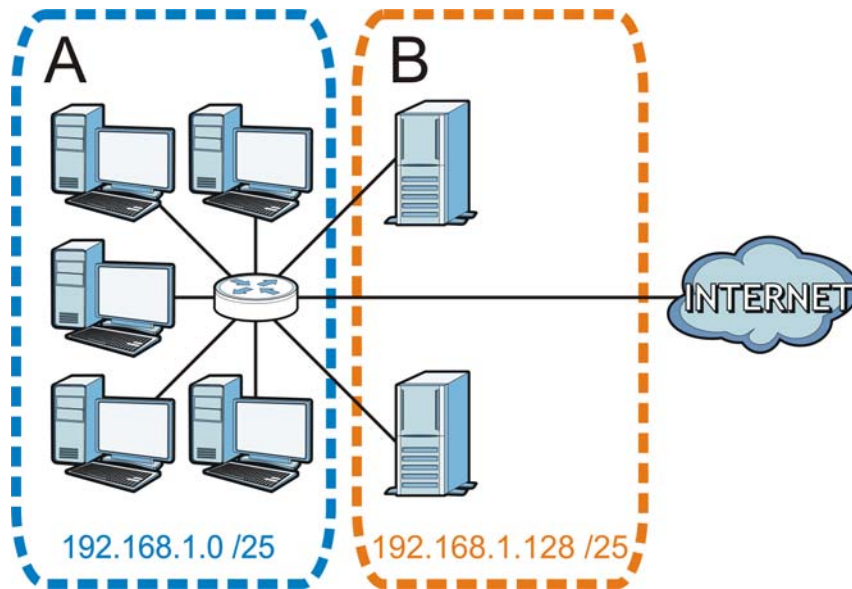
Figure 109 Subnetting Example: Before Subnetting

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 110 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 |

Table 71 Subnet 1 (continued)

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|------------------------------------|-------------------------------|----------------------|
| 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 |
| 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 |

Table 77 16-bit Network Number Subnet Planning (continued)

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|--------------------------|-----------------------|-------------|----------------------|
| 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 NBG4104.

Once you have decided on the network number, pick an IP address for your NBG4104 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 NBG4104 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 NBG4104 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.

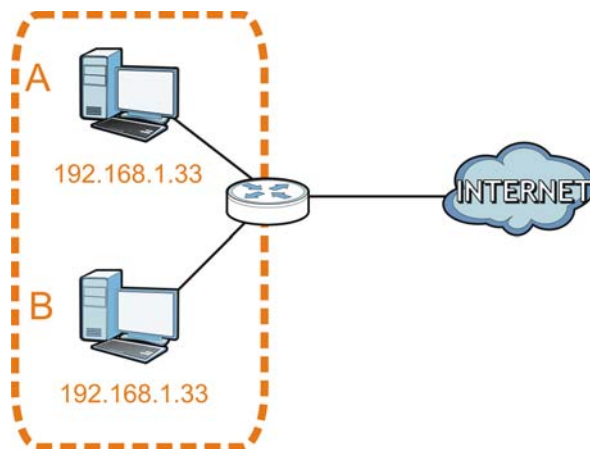
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

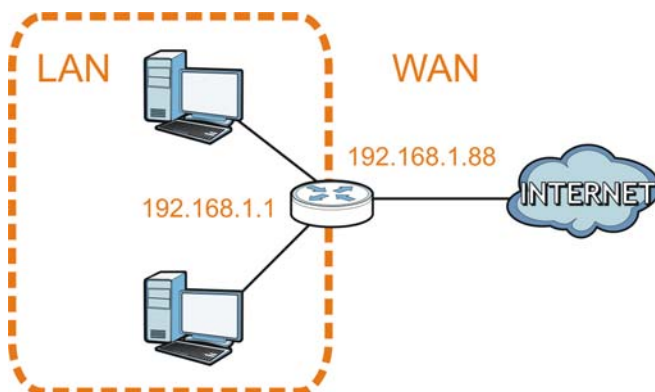
Figure 111 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

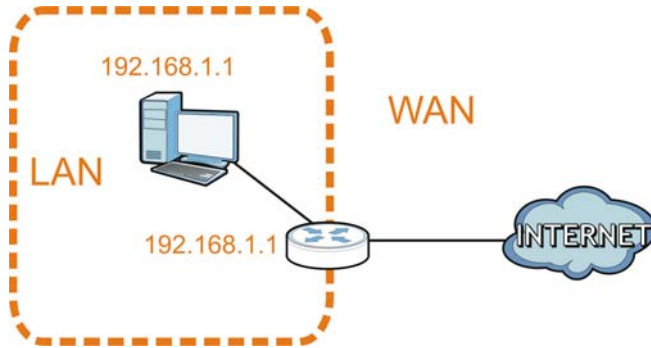
Figure 112 Conflicting Router IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 113 Conflicting Computer and Router IP Addresses Example



Setting Up Your Computer's IP Address

Note: Your specific NBG4104 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

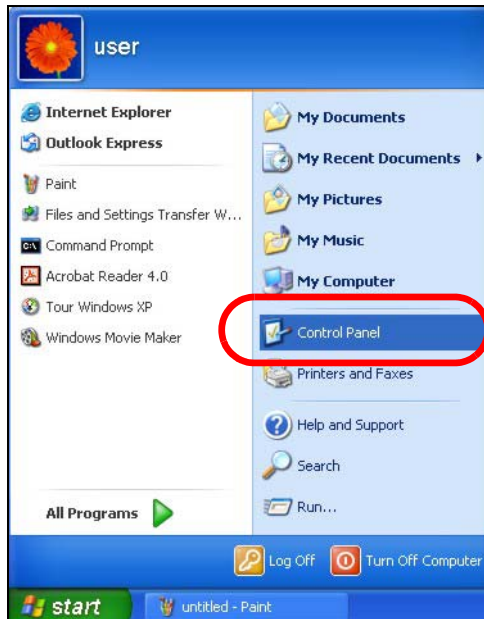
In this appendix, you can set up an IP address for:

- [Windows XP/NT/2000 on page 186](#)
- [Windows Vista on page 189](#)
- [Windows 7 on page 193](#)
- [Mac OS X: 10.3 and 10.4 on page 197](#)
- [Mac OS X: 10.5 and 10.6 on page 200](#)
- [Linux: Ubuntu 8 \(GNOME\) on page 203](#)
- [Linux: openSUSE 10.3 \(KDE\) on page 207](#)

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

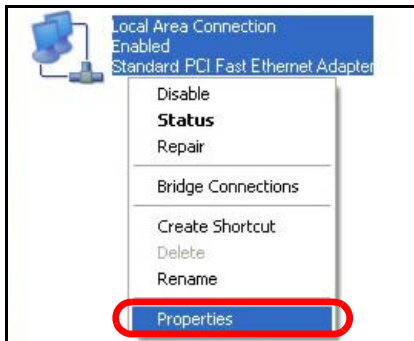
- 1 Click **Start > Control Panel**.



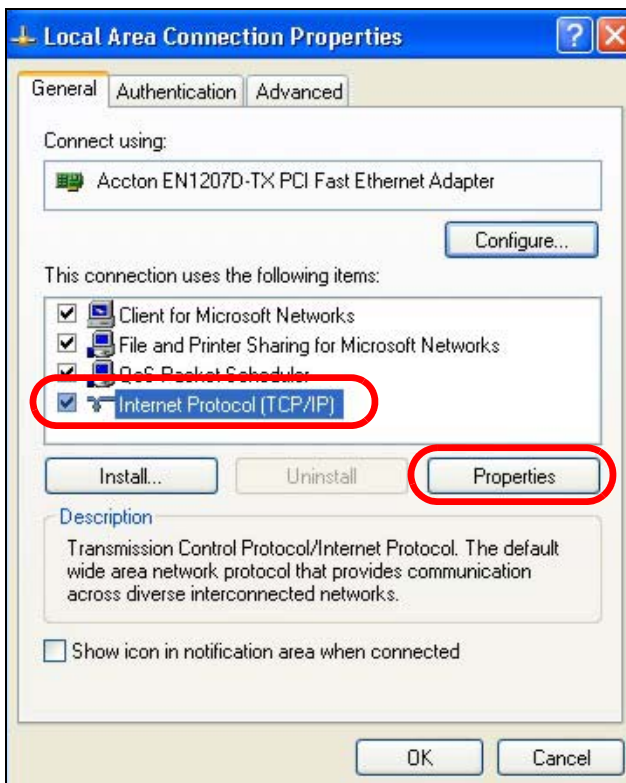
- 2 In the **Control Panel**, click the **Network Connections** icon.



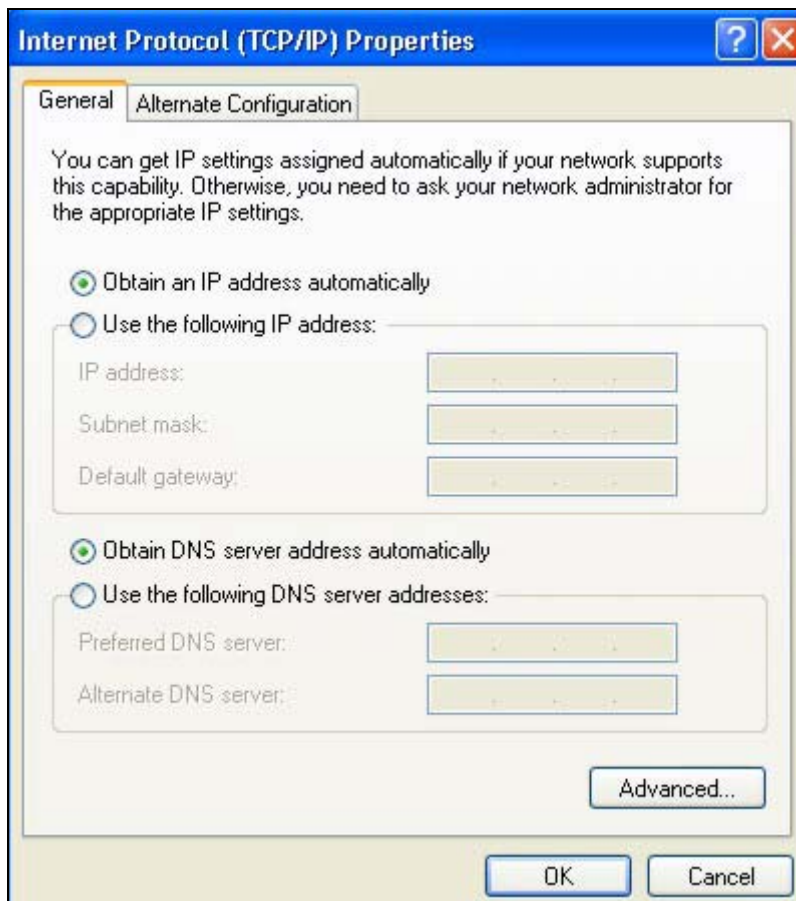
- 3 Right-click **Local Area Connection** and then select **Properties**.



- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



- 5 The **Internet Protocol TCP/IP Properties** window opens.



- 6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

- 7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

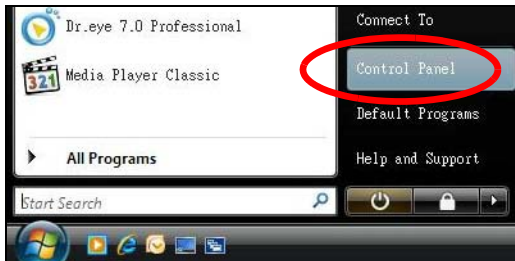
- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

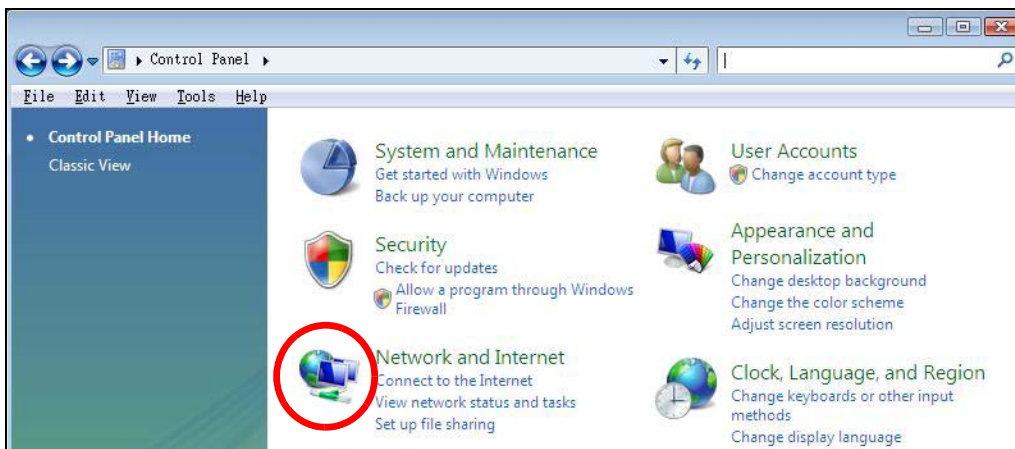
Windows Vista

This section shows screens from Windows Vista Professional.

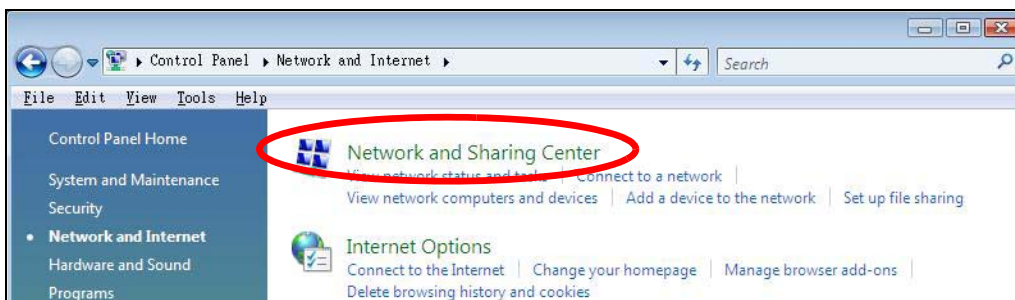
- 1 Click **Start > Control Panel**.



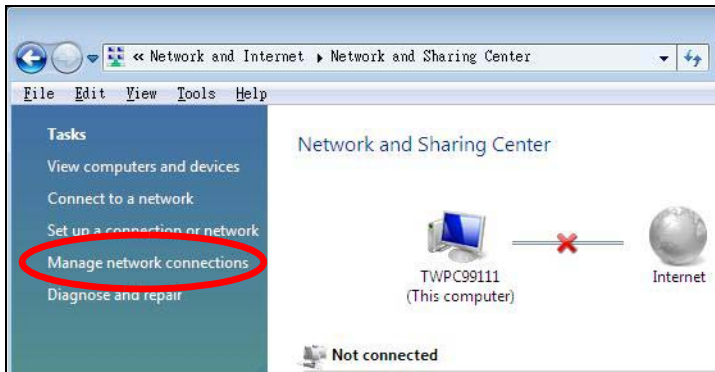
- 2 In the **Control Panel**, click the **Network and Internet** icon.



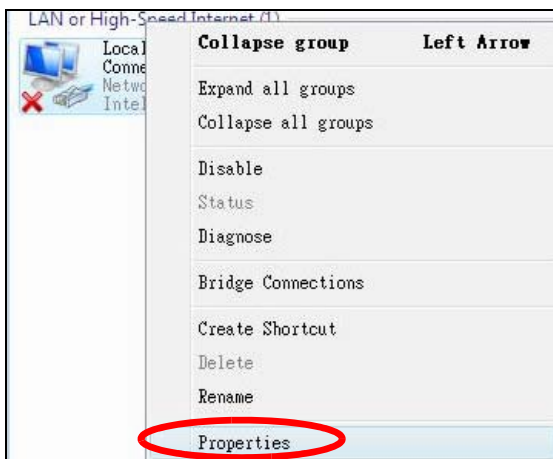
- 3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

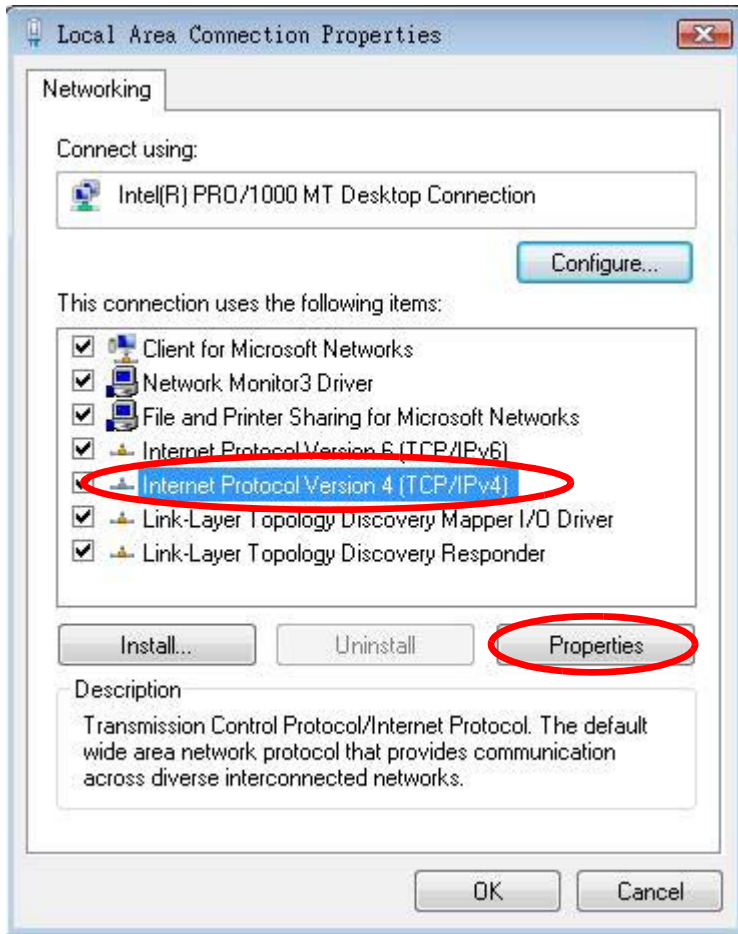


5 Right-click **Local Area Connection** and then select **Properties**.

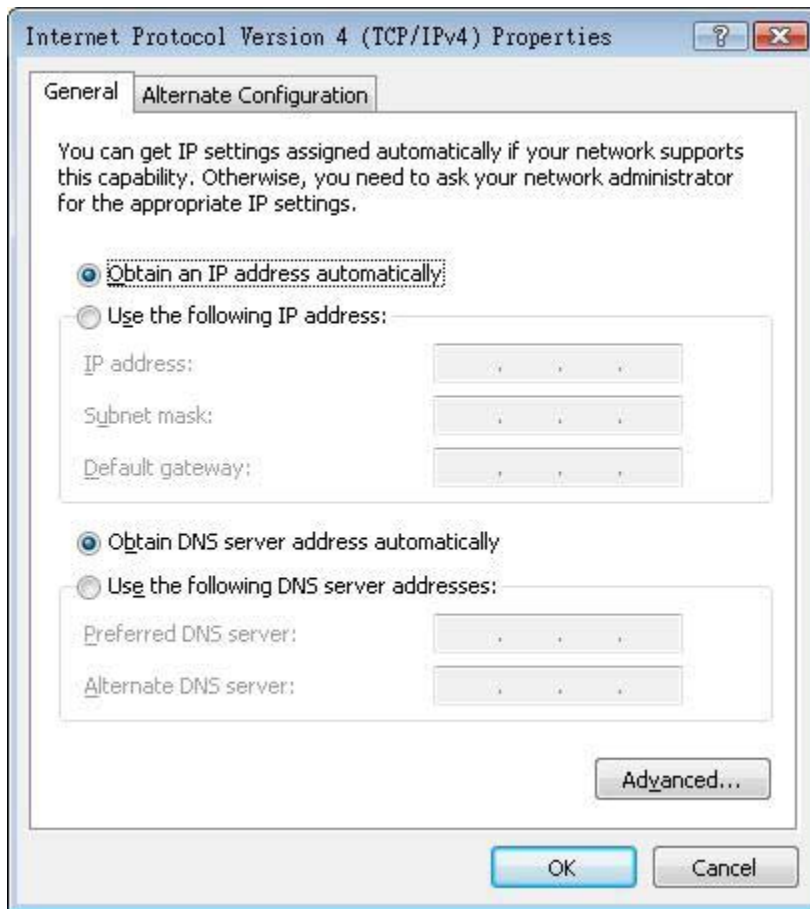


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



- 8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.
Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced**.
- 9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 10 Click **OK** to close the **Local Area Connection Properties** window.

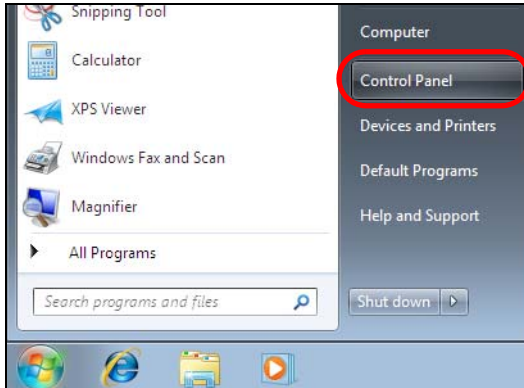
Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

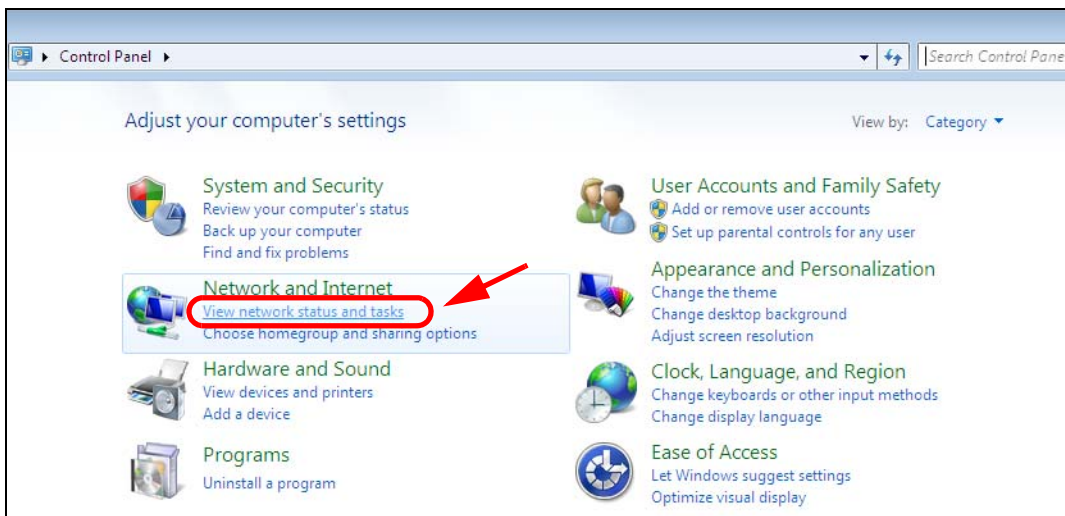
Windows 7

This section shows screens from Windows 7 Enterprise.

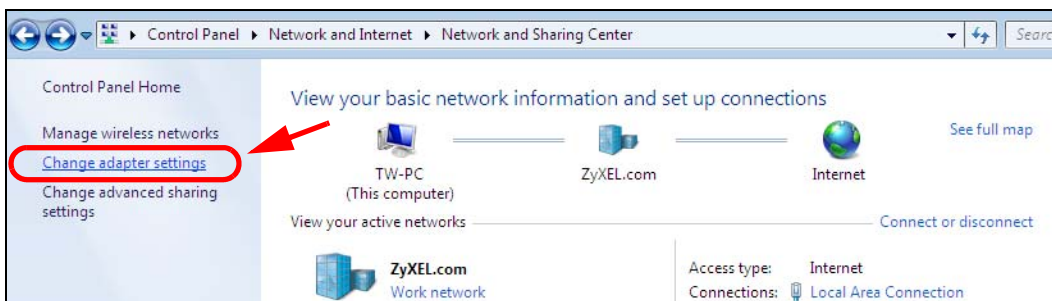
- 1 Click **Start > Control Panel**.



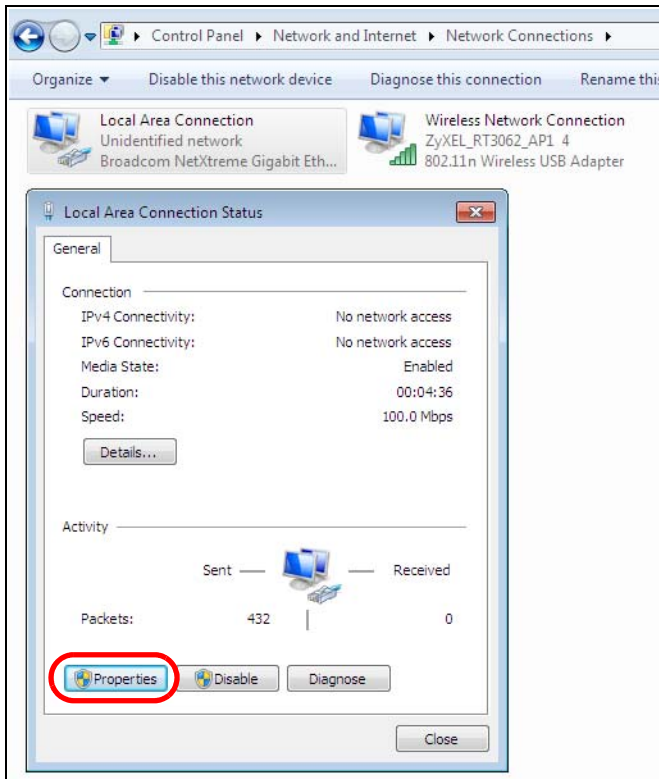
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



- 3 Click **Change adapter settings**.

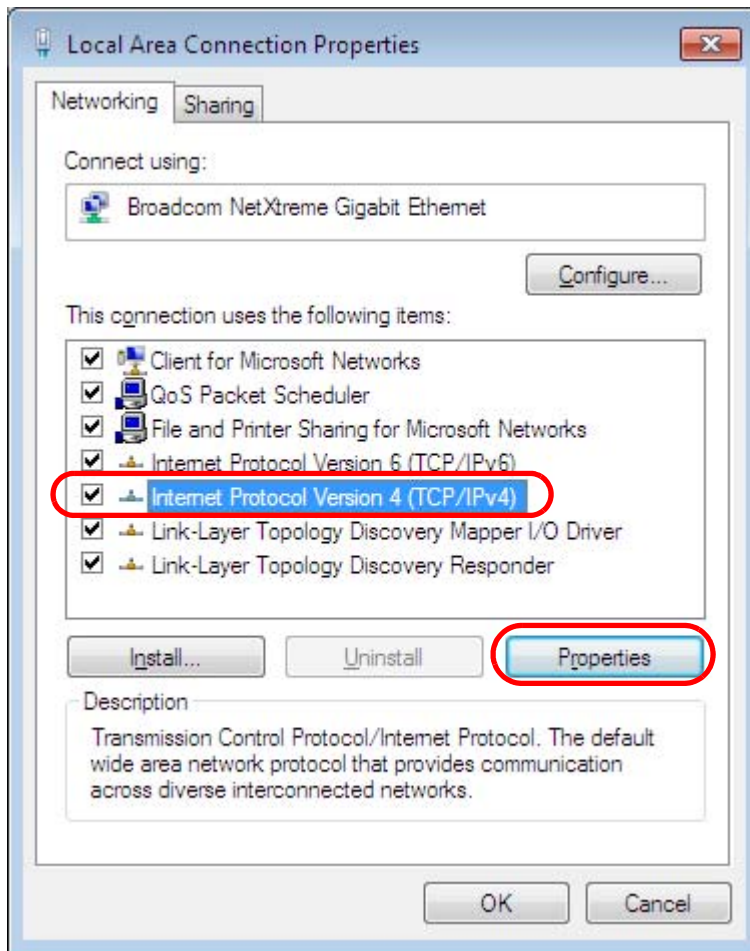


- 4 Double click **Local Area Connection** and then select **Properties**.

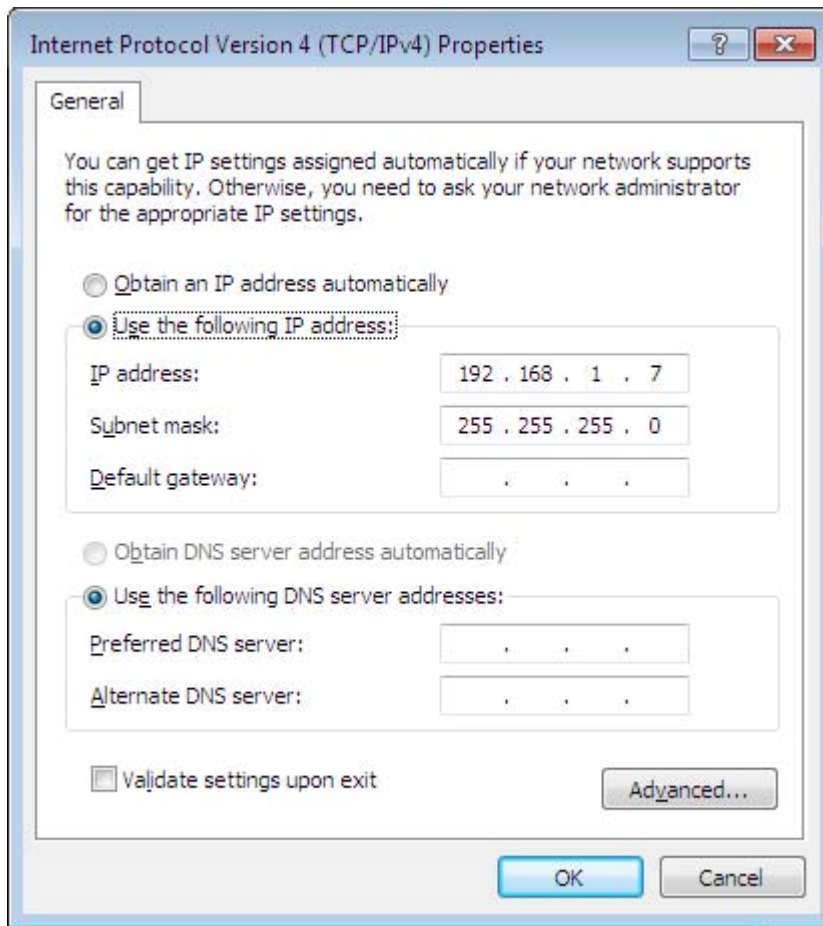


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



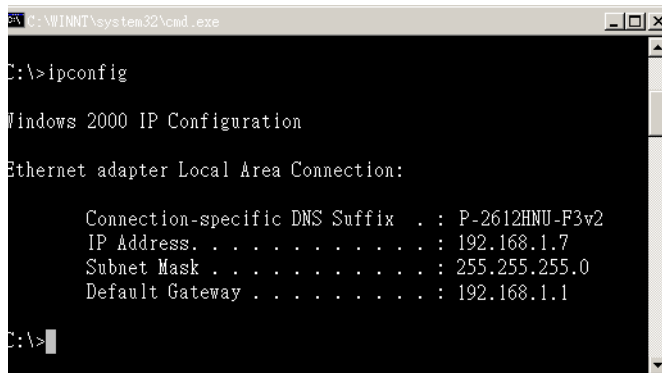
- The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



- Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.
Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.
- Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].
- 3 The IP settings are displayed as follows.



```
C:\WINNT\system32\cmd.exe
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

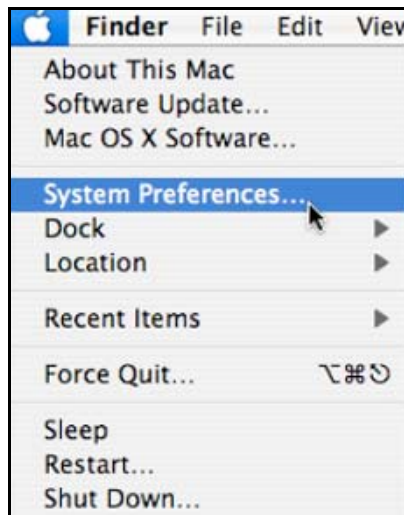
    Connection-specific DNS Suffix  . : P-2612HNU-F3v2
    IP Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>
```

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

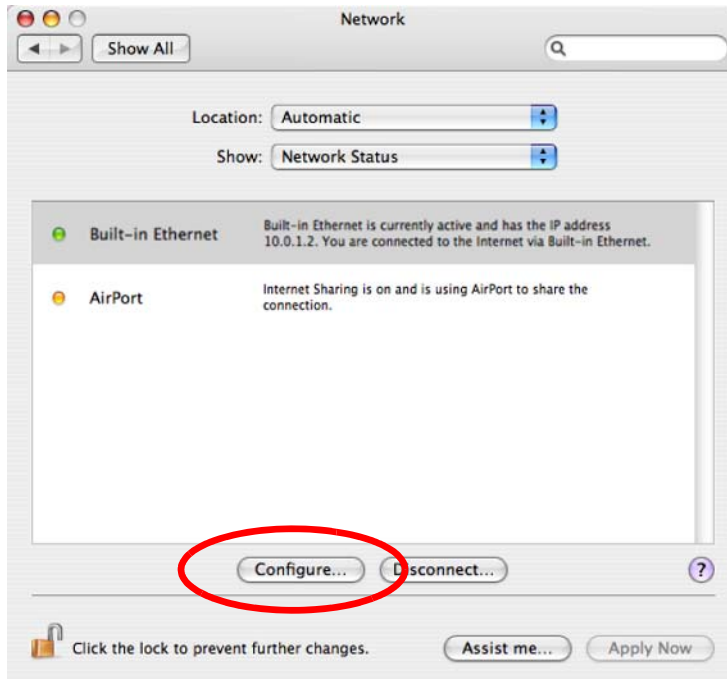
- 1 Click **Apple > System Preferences**.



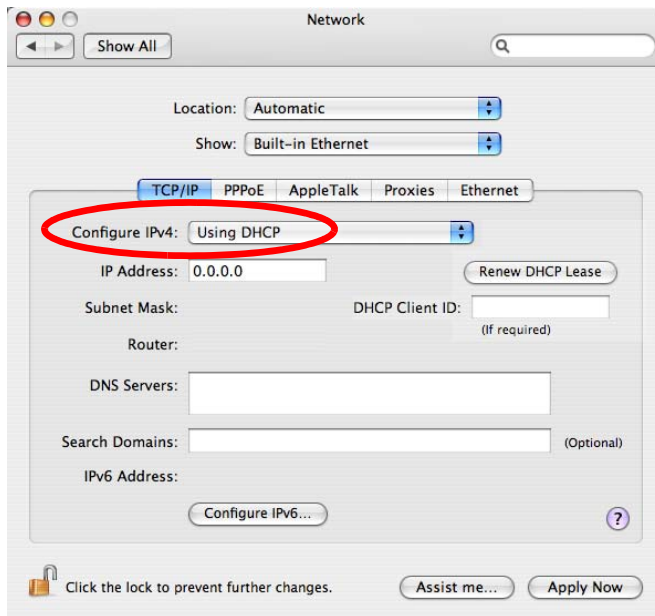
- 2 In the **System Preferences** window, click the **Network** icon.



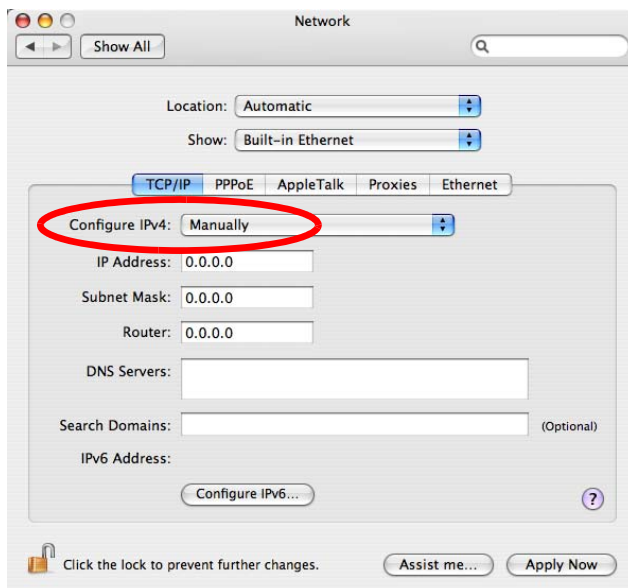
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.



- For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



- For statically assigned settings, do the following:
 - From the **Configure IPv4** list, select **Manually**.
 - In the **IP Address** field, type your IP address.
 - In the **Subnet Mask** field, type your subnet mask.
 - In the **Router** field, type the IP address of your device.

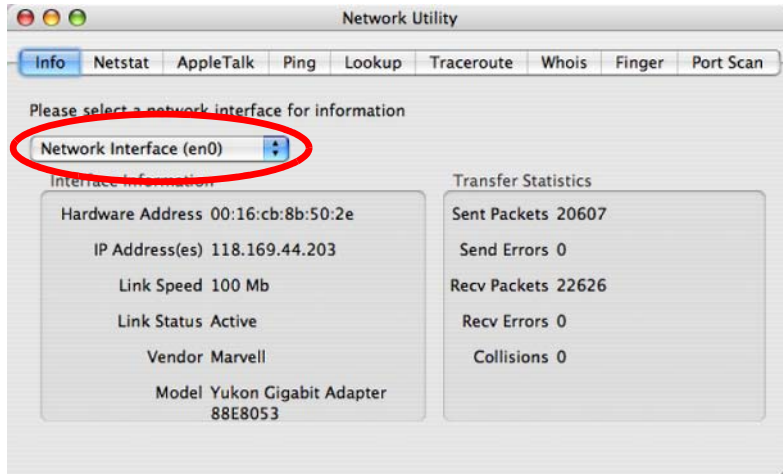


- Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

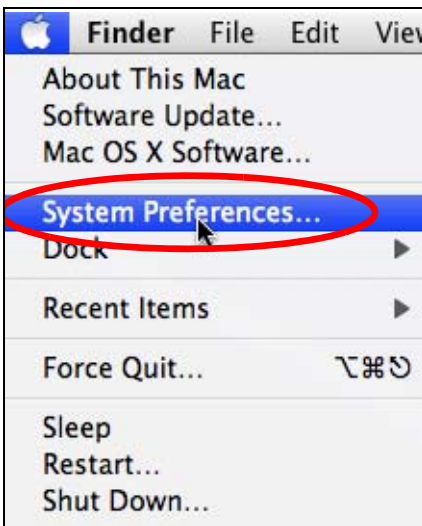
Figure 114 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

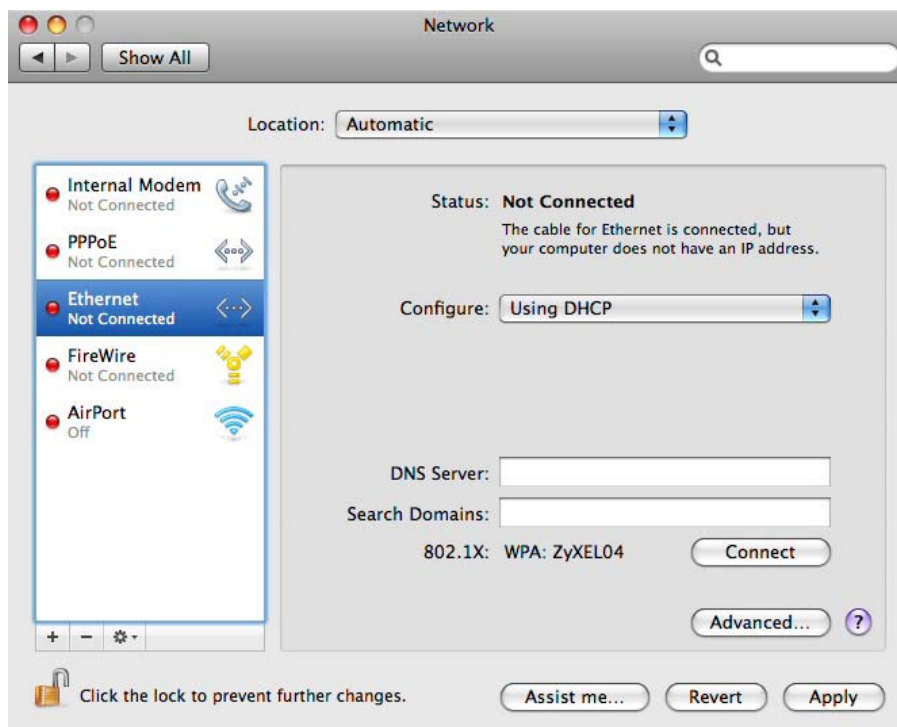
- 1 Click **Apple > System Preferences**.



- 2 In **System Preferences**, click the **Network** icon.

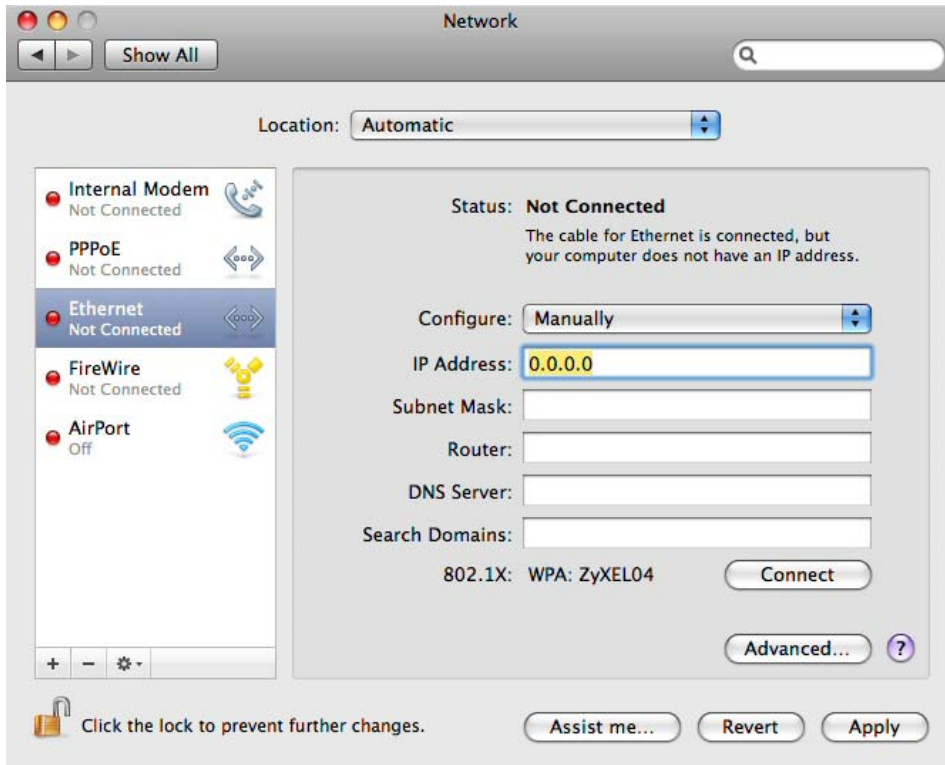


- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



- 4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

- 5 For statically assigned settings, do the following:
 - From the **Configure** list, select **Manually**.
 - In the **IP Address** field, enter your IP address.
 - In the **Subnet Mask** field, enter your subnet mask.
 - In the **Router** field, enter the IP address of your NBG4104.

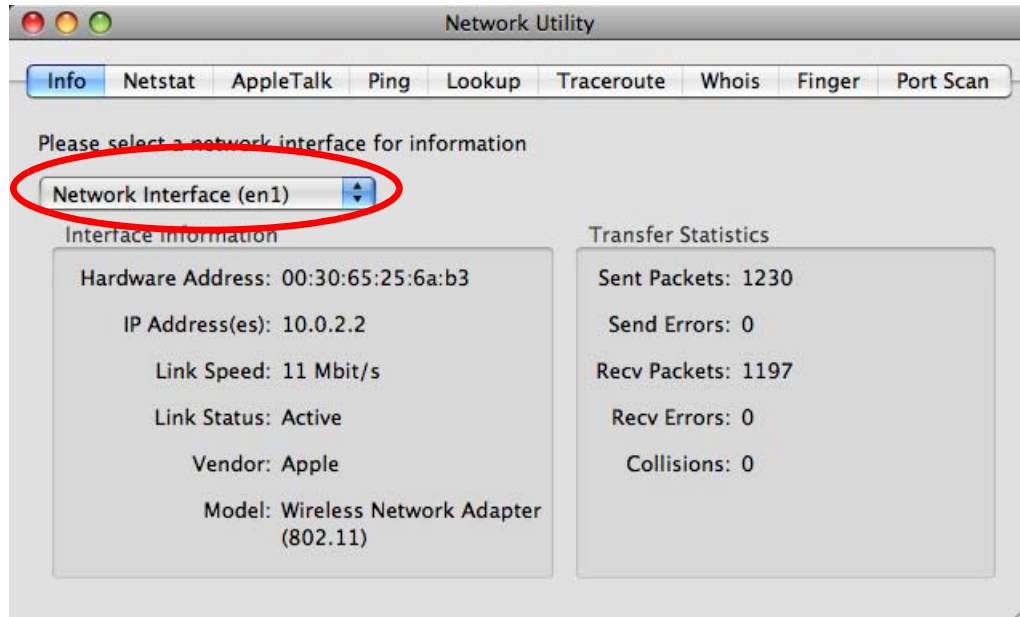


- 6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 115 Mac OS X 10.5: Network Utility



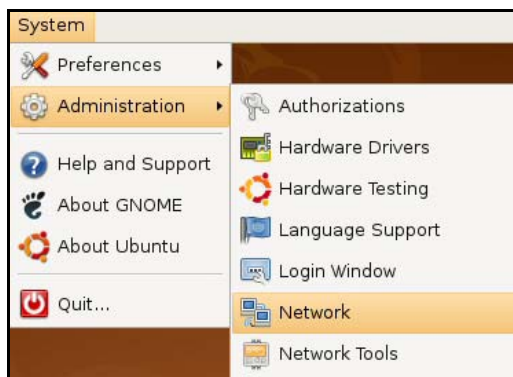
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

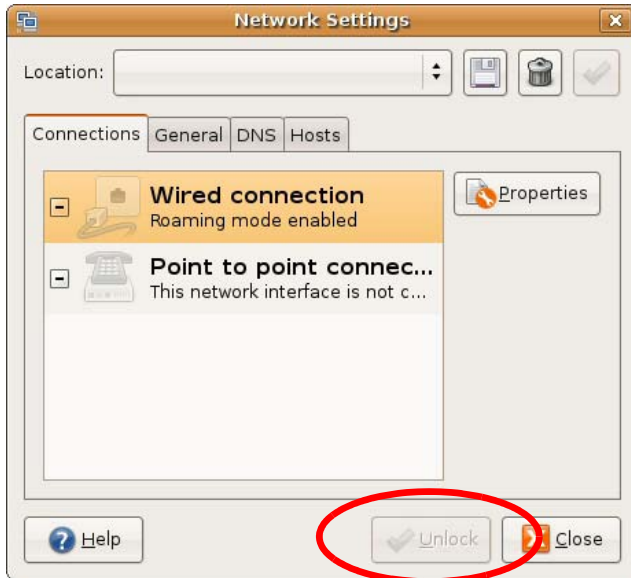
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

- 1 Click **System > Administration > Network**.



- When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



- In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.



- 4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.



- 5 The **Properties** dialog box opens.



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
 - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

- 7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

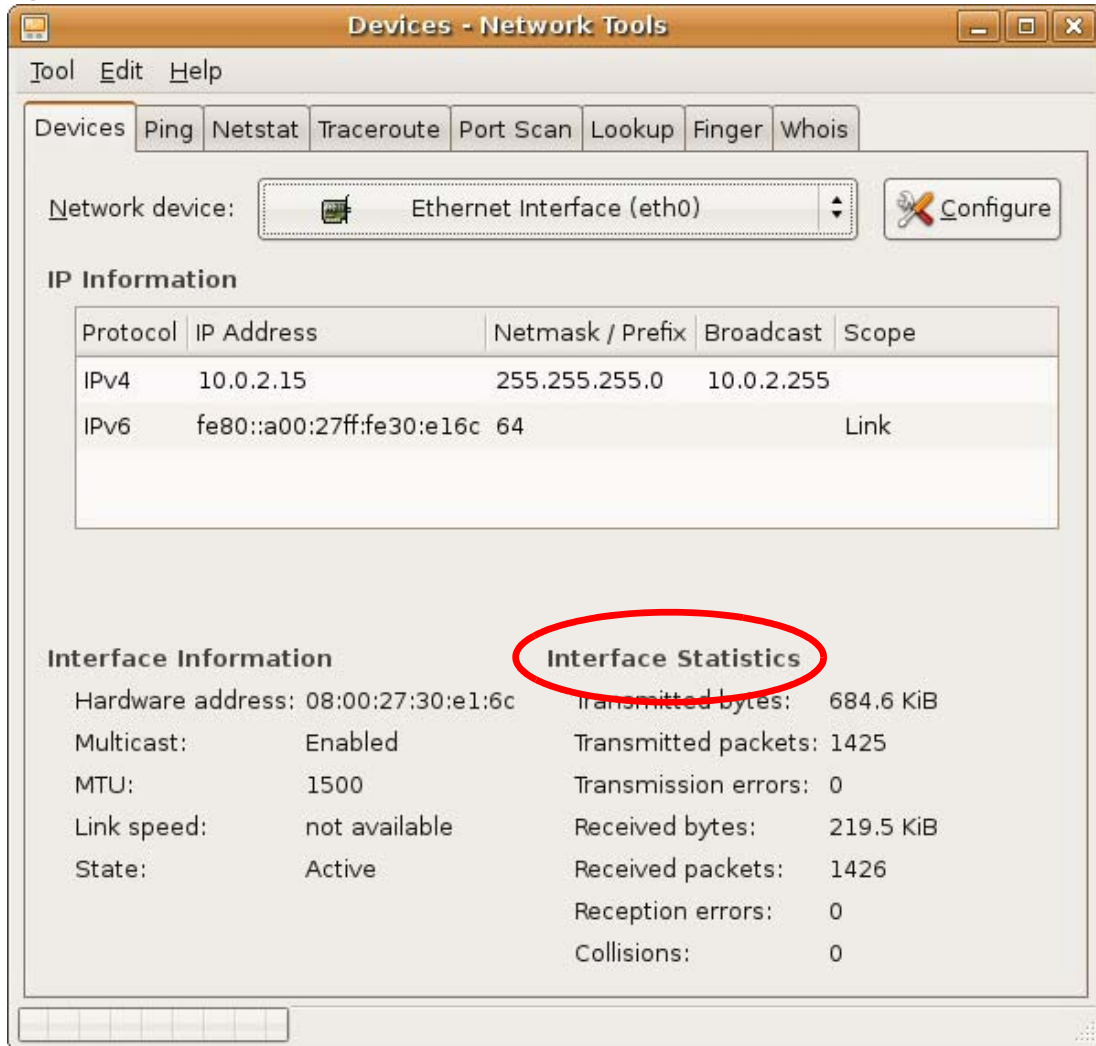


- 8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 116 Ubuntu 8: Network Tools



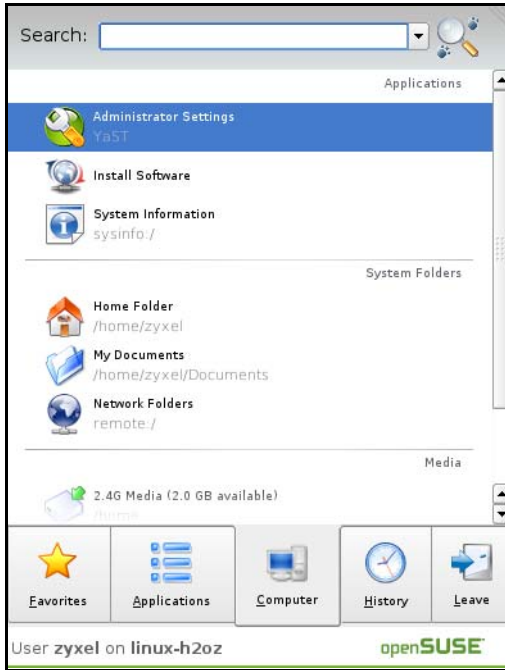
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

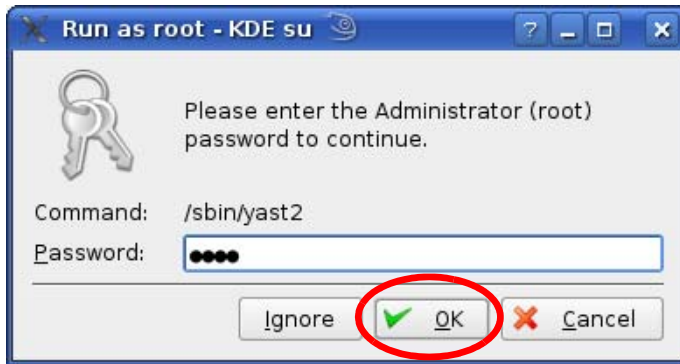
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

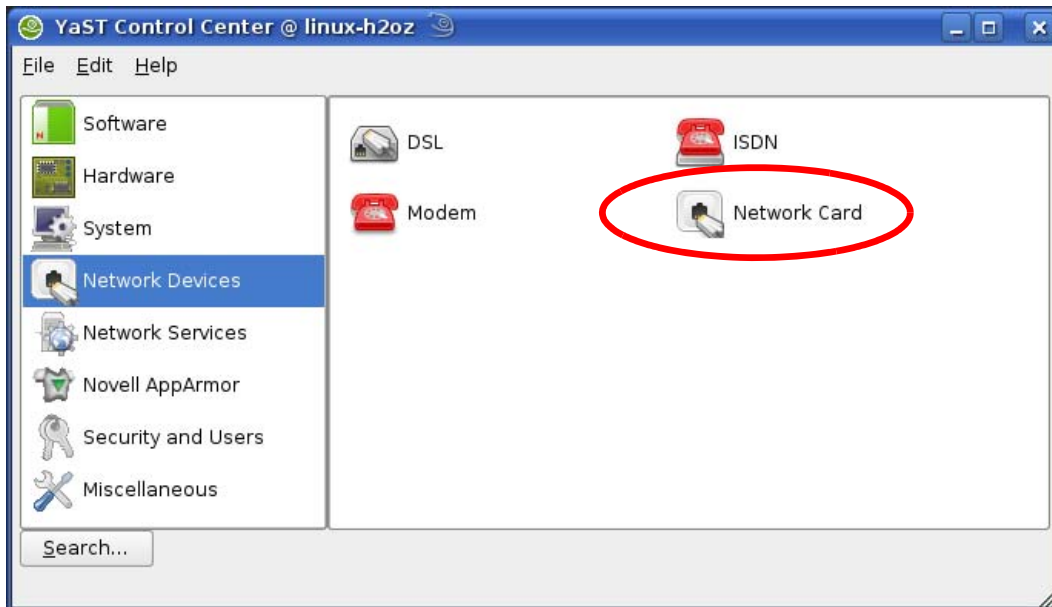
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.



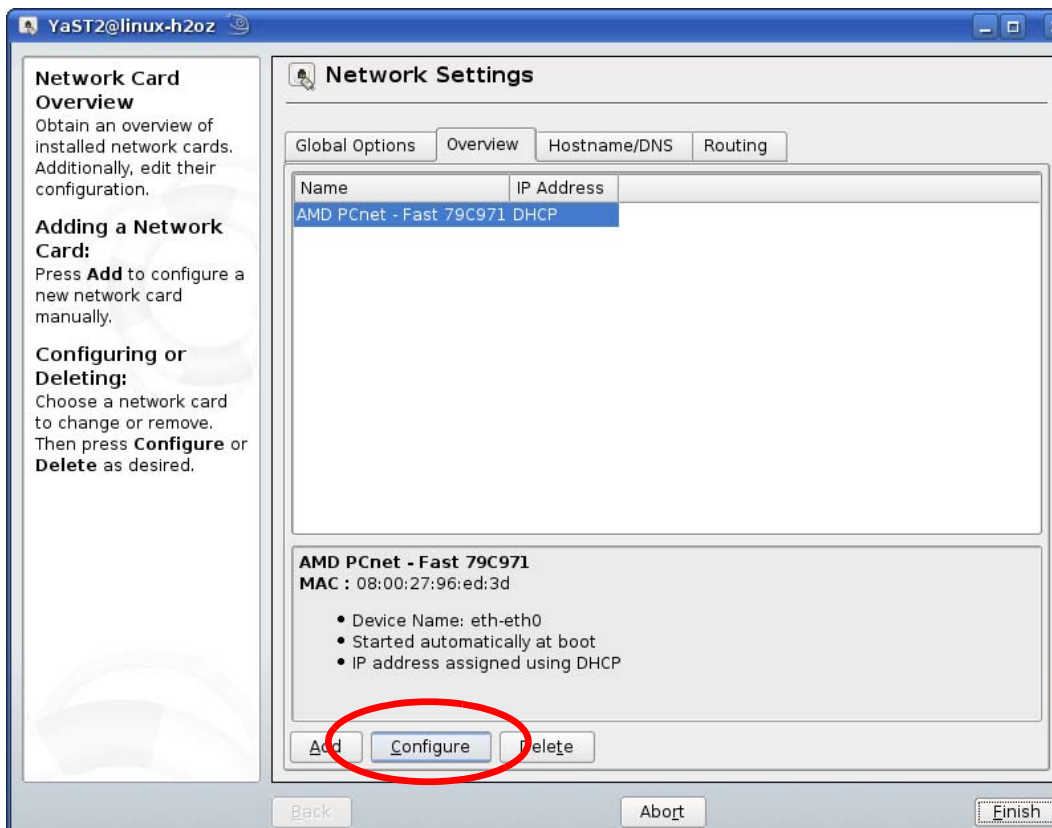
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.



- When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

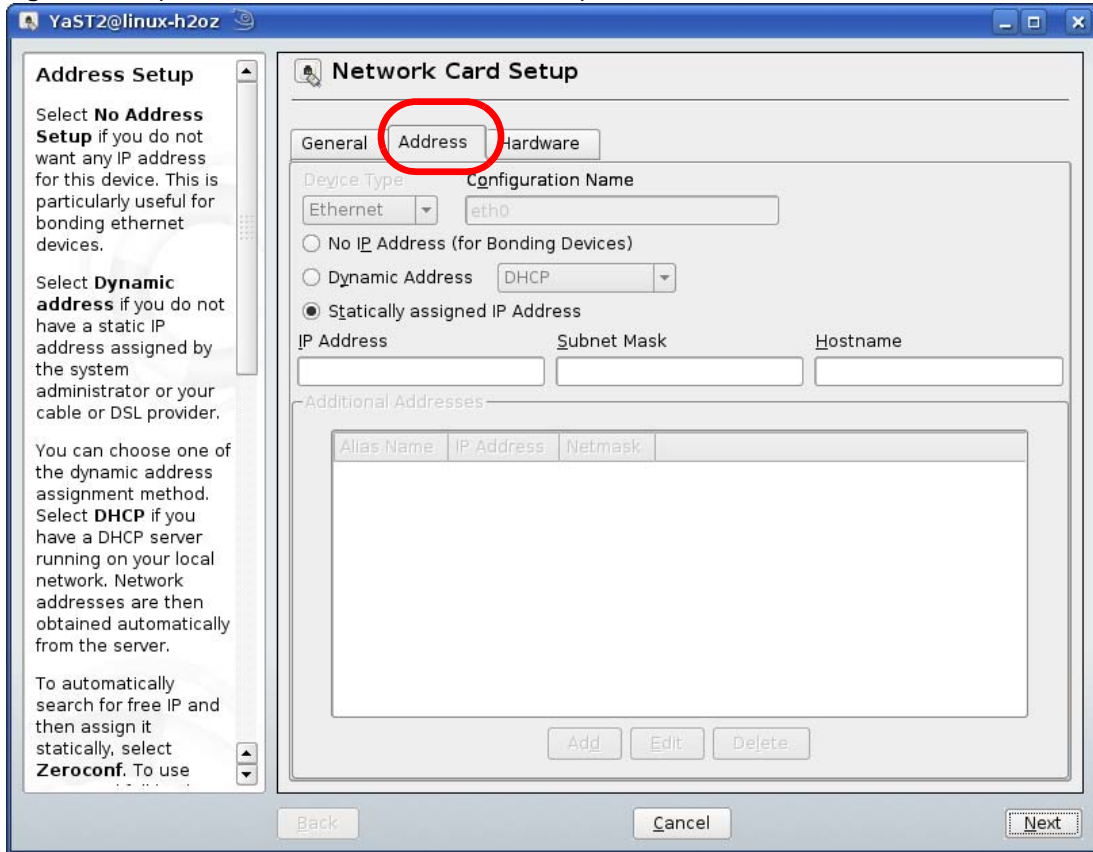


- When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



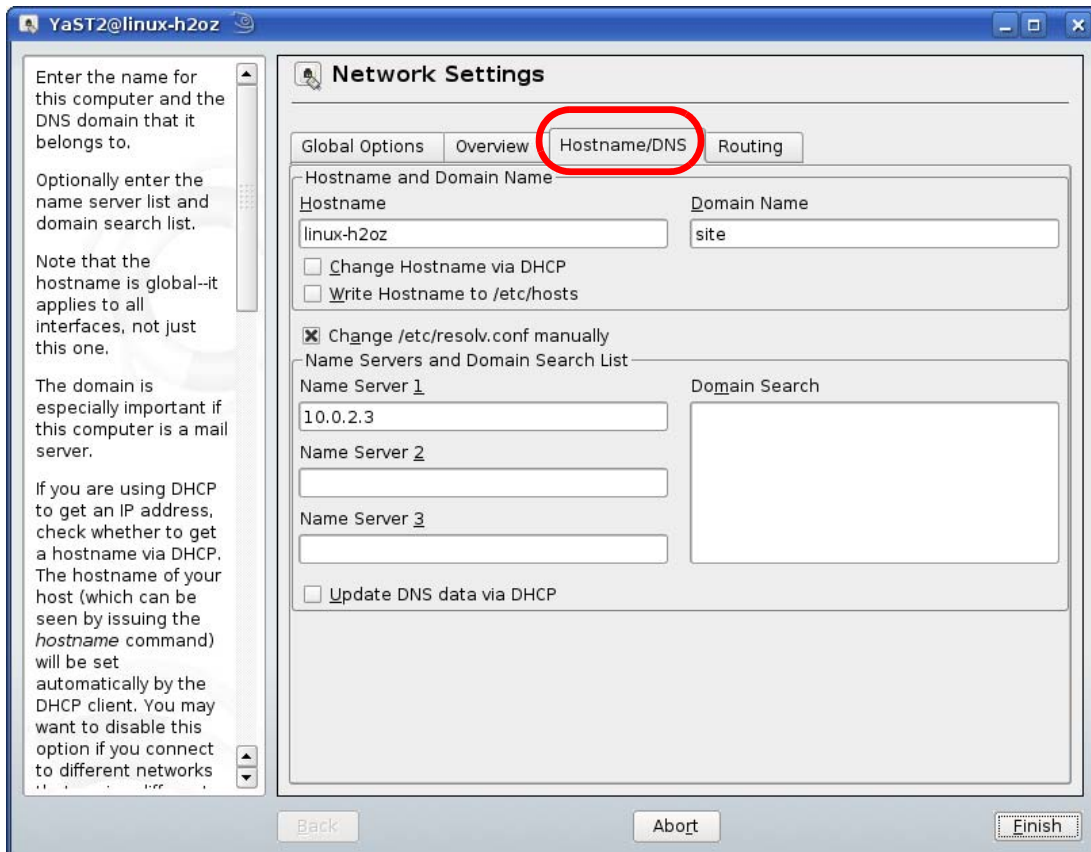
- When the **Network Card Setup** window opens, click the **Address** tab

Figure 117 openSUSE 10.3: Network Card Setup



- Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- Click **Next** to save the changes and close the **Network Card Setup** window.

- 8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

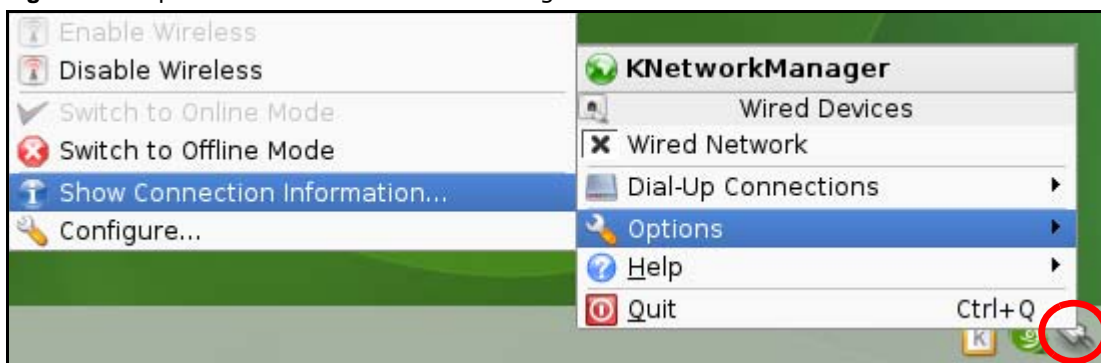


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

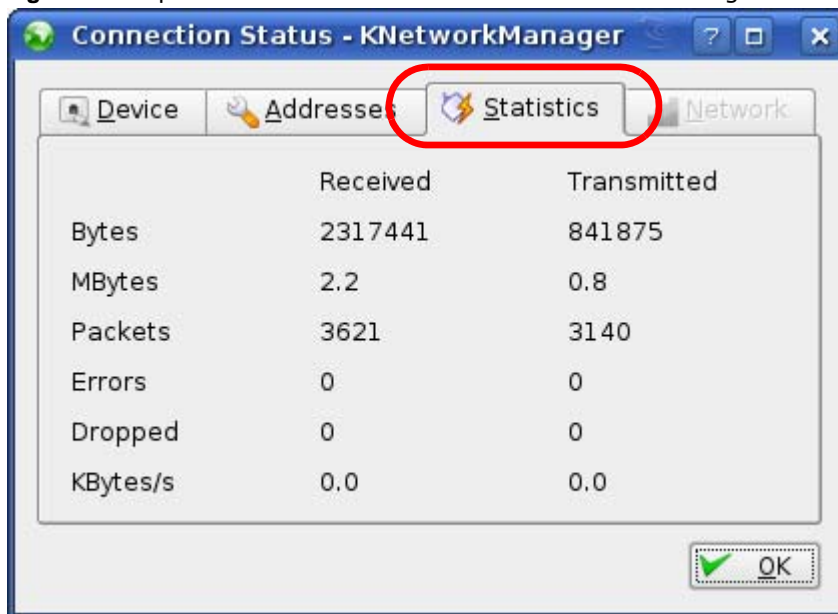
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 118 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics** tab to see if your connection is working properly.

Figure 119 openSUSE: Connection Status - KNetwork Manager



Wireless LANs

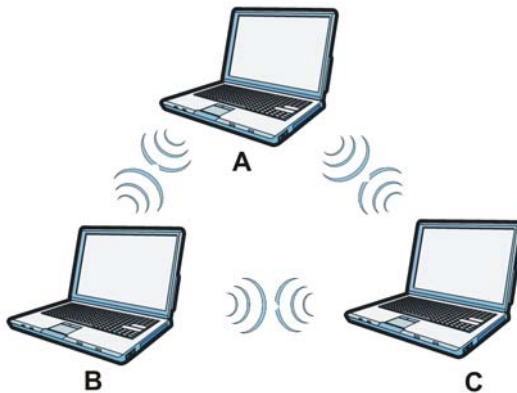
Wireless LAN Topologies

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 adapters (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 120 Peer-to-Peer Communication in an Ad-hoc Network



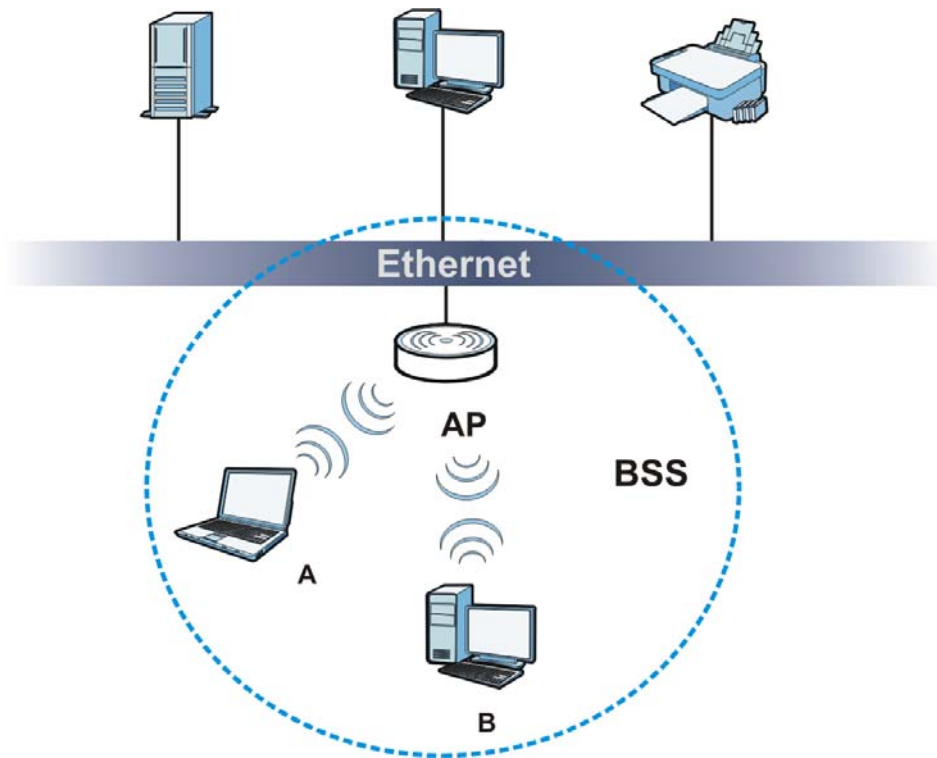
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **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.

Figure 121 Basic Service Set



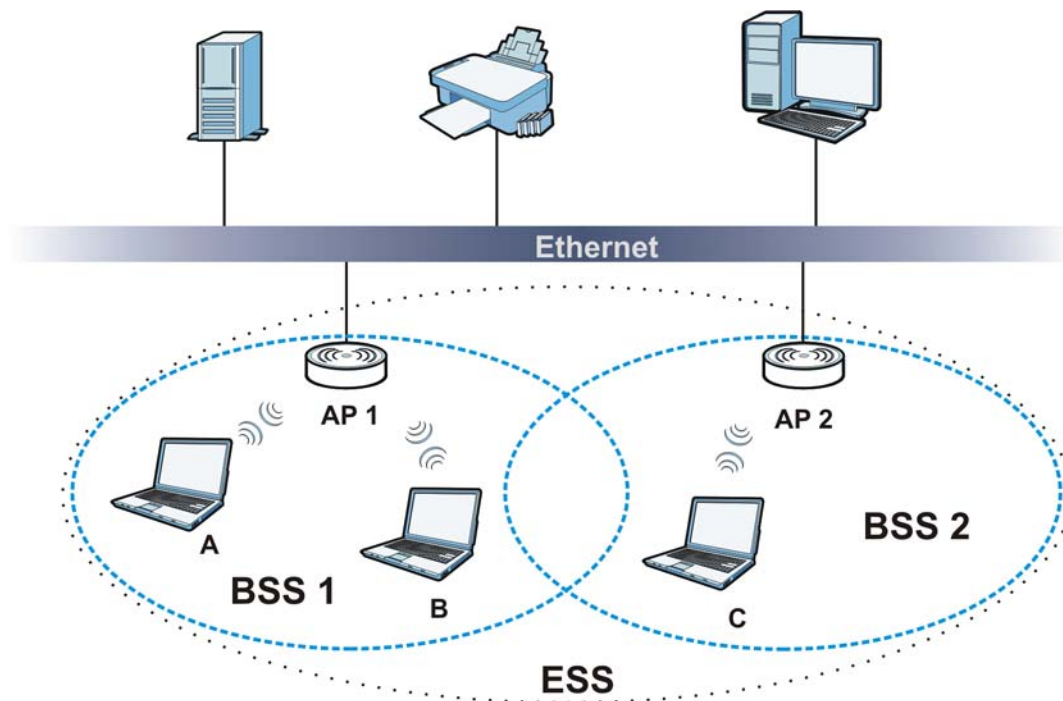
ESS

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 clients within the same ESS must have the same ESSID in order to communicate.

Figure 122 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

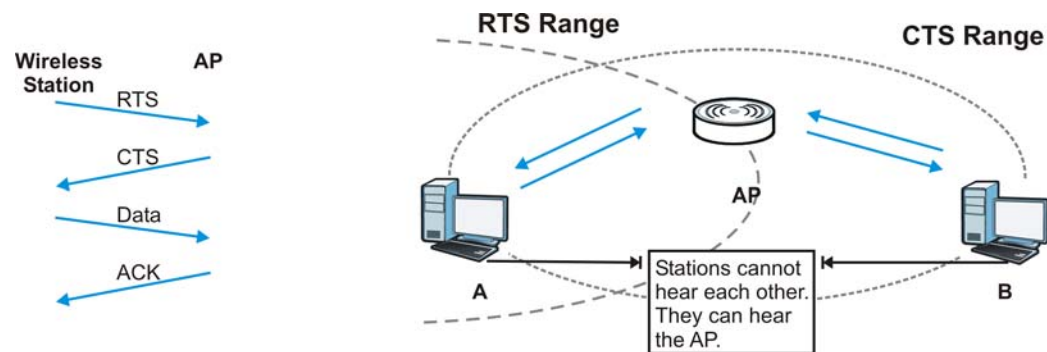
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel 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 123 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

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NBG4104 uses long preamble.

Note: The wireless devices **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) |

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the NBG4104 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NBG4104 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NBG4104.

Table 79 Wireless Security Levels

| SECURITY LEVEL | SECURITY TYPE |
|----------------|--|
| Least Secure | Unique SSID (Default) |
| | Unique SSID with Hide SSID Enabled |
| | MAC Address Filtering |
| | WEP Encryption |
| | IEEE802.1x EAP with RADIUS Server Authentication |
| | Wi-Fi Protected Access (WPA) |
| Most Secure | WPA2 |

Note: You must enable the same wireless security settings on the NBG4104 and on all wireless clients that you want to associate with it.

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 clients.

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 client 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 EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client '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 clients 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 security configuration screen. You may still configure and store keys, 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 80 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 and WPA2

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 or WPA2 and WEP are improved data encryption and user authentication.

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.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm

called Rijndael. They both include 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.

WPA and WPA2 regularly change and rotate 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 PMK 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.

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), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevents all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go through the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

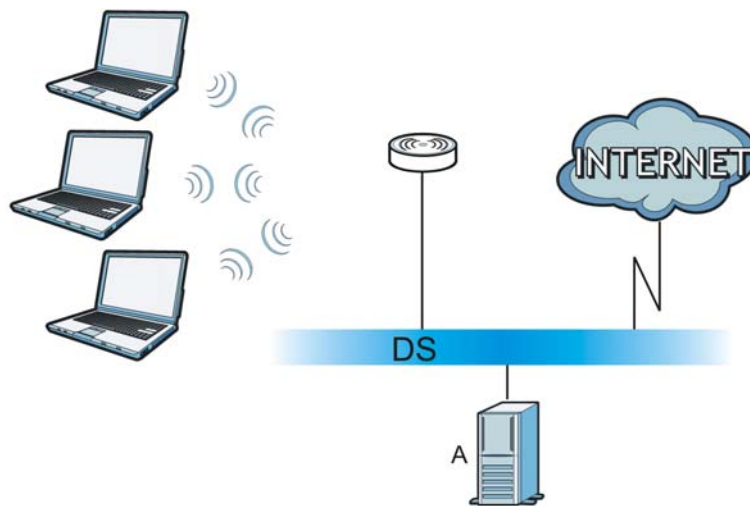
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), 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 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 124 WPA(2) with RADIUS Application Example



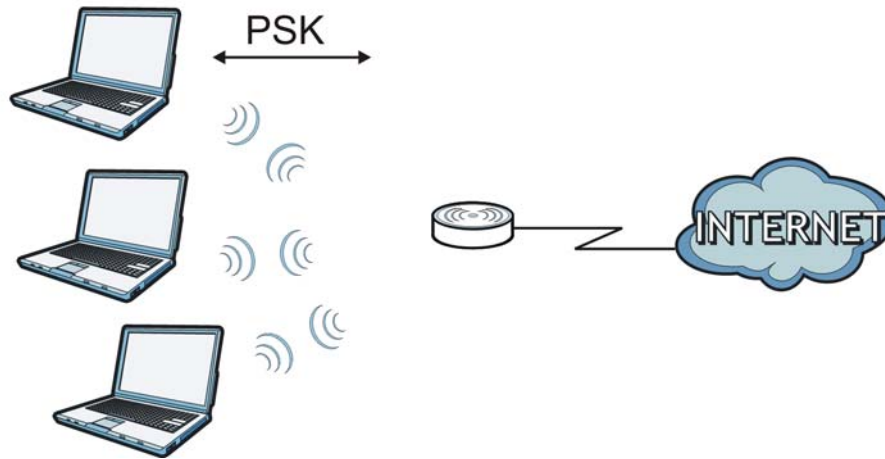
WPA(2)-PSK Application Example

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 or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 125 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 81 Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTIO N METHOD | ENTER MANUAL KEY | IEEE 802.1X |
|--|--------------------|------------------|--------------------------------|
| Open | None | No | Disable |
| | | Yes | 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/AES | No | Enable |
| WPA-PSK | TKIP/AES | Yes | Disable |
| WPA2 | TKIP/AES | No | Enable |
| WPA2-PSK | TKIP/AES | Yes | Disable |

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
 - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 82 Commonly Used Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|--------------------|--------------|---------------|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM/New-ICQ | TCP | 5190 | AOL's Internet Messenger service. It is also used as a listening port by ICQ. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP UDP | 7648 24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for example 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. |
| | TCP TCP | 20 21 | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |

Table 82 Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|-------------------|--------------|---------|--|
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic or routing purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Management Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| S | TCP | 115 | Simple File Transfer Protocol. |

Table 82 Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|------------|----------|---------|--|
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| T | UDP | 69 | Trivial File Transfer Protocol is an Internet file transfer protocol similar to , but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE | TCP | 7000 | Another videoconferencing solution. |

Legal Information

Copyright

Copyright © 2011 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

NetUSB is a 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 and 5dBi.

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.

End-User License Agreement

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1 Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3 Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or

otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL on its Open Source web site (://opensource.zyxel.com) (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (://opensource.zyxel.com), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE,

OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyxEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyxEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8 Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyxEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9 Audit Rights

ZyxEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10 Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyxEL all copies of the Software and Documentation in your possession or under your control. ZyxEL may terminate this License Agreement for any reason, including, but not limited to, if ZyxEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyxEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyxEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: Some components of this product incorporate source code covered under the Apache License, GPL License, LGPL License, Sun License, and Castor License. To obtain the source code covered under those Licenses, please check ://
opensource.zyxel.com to get it.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

| | |
|--------------|---|
| [Czech] | ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC. |
| [Danish] | Undertegnede ZyXEL erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. |
| [German] | Hiermit erkläre ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet. |
| [Estonian] | Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. |
| English | Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. |
| [Spanish] | Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE. |
| [Greek] | ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΖΥΧΕΛ ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ. |
| [French] | Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC. |
| [Italian] | Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE. |
| [Latvian] | Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. |
| [Lithuanian] | Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas. |
| [Dutch] | Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC. |
| [Maltese] | Hawnhekk, ZyXEL, jiddikjara li dan taghmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC. |
| [Hungarian] | Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak. |
| [Polish] | Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC. |
| [Portuguese] | ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC. |

| | |
|-------------|--|
| [Slovenian] | ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC. |
| [Slovak] | ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC. |
| [Finnish] | ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
| [Swedish] | Härmed intygar ZyXEL att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC. |
| [Bulgarian] | С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC. |
| [Icelandic] | Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC. |
| [Norwegian] | Erklærer herved ZyXEL at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 1999/5/EF. |
| [Romanian] | Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/EC. |



National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Ausnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "Overview of Regulatory Requirements for Wireless LANs":.

| Overview of Regulatory Requirements for Wireless LANs | | | |
|---|---|-------------|--------------------|
| Frequency Band (MHz) | Max Power Level (EIRP) ¹ (mW) | Indoor ONLY | Indoor and Outdoor |
| | | | |

| | | | |
|-------------|------|---|---|
| 2400-2483.5 | 100 | | V |
| 5150-5350 | 200 | V | |
| 5470-5725 | 1000 | | V |

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check <http://www.arcep.fr/> for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez <http://www.arcep.fr/> pour de plus amples détails.

| | | |
|--------------------------|----------------------|---------------|
| R&TTE 1999/5/EC | | |
| WLAN 2.4 – 2.4835 GHz | | |
| IEEE 802.11 b/g/n | | |
| Location | Frequency Range(GHz) | Power (EIRP) |
| Indoor (No restrictions) | 2.4 – 2.4835 | 100mW (20dBm) |
| Outdoor | 2.4 – 2.454 | 100mW (20dBm) |
| | 2.454 – 2.4835 | 10mW (10dBm) |

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check <http://www.sviluppoeconomico.gov.it/> for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio

fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <http://www.sviluppoeconomico.gov.it/> per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <http://www.esd.lv> for more details.

2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <http://www.esd.lv>.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Index

A

ActiveX [118](#)
Address Assignment [70](#)
Advanced Encryption Standard
 See AES.
AES [221](#)
alternative subnet mask notation [177](#)
antenna
 directional [225](#)
 gain [225](#)
 omni-directional [225](#)
AP [17](#)
AP (access point) [215](#)
AP Mode
 menu [42](#)
 status screen [40](#)
AP+Bridge [17](#)

B

Bandwidth management
 overview [130](#)
Basic Service Set, See BSS [213](#)
Bridge/Repeater [17](#)
BSS [213](#)

C

CA [220](#)
Certificate Authority
 See CA.
certifications [231](#)
 notices [233](#)
 viewing [233](#)
Channel [34, 41](#)
channel [56, 215](#)
 interference [215](#)

Configuration
 restore [148](#)
content filtering [117](#)
 by keyword (in URL) [117](#)
Cookies [118](#)
copyright [231](#)
CPU usage [34, 41](#)
CTS (Clear to Send) [216](#)

D

DDNS [95](#)
 see also Dynamic DNS
 service providers [96](#)
DHCP [26, 85](#)
 DHCP server
 see also Dynamic Host Configuration Protocol
DHCP server [82, 85](#)
DHCP table [27](#)
 DHCP client information
 DHCP status
Dimensions [159](#)
disclaimer [231](#)
DNS [87](#)
DNS Server [70](#)
DNS server [87](#)
Domain Name System [87](#)
Domain Name System. See DNS.
duplex setting [35, 41](#)
Dynamic DNS [95](#)
Dynamic Host Configuration Protocol [85](#)
dynamic WEP key exchange [220](#)
DynDNS [96](#)
DynDNS see also DDNS [96](#)
DynDNS Wildcard [95](#)

E

EAP Authentication [219](#)
encryption [57, 221](#)
 and local (user) database [58](#)
 key [58](#)
 WPA compatible [58](#)
ESS [214](#)
ESSID [155](#)
Extended Service Set, See ESS [214](#)

F

FCC interference statement [231](#)
Firewall [112](#)
 Firewall overview
 guidelines [112](#)
 network security
 Stateful inspection [112](#)
 ZyXEL device firewall [112](#)
firewall
 stateful inspection [111](#)
Firmware upload [146](#)
 file extension
 using HTTP
firmware version [34, 40](#)
fragmentation threshold [216](#)

G

General wireless LAN screen [58](#)
Guest WLAN [59](#)

H

hidden node [215](#)

I

IANA [182](#)

IBSS [213](#)
IEEE 802.11g [217](#)
IGMP [71](#)
 see also Internet Group Multicast Protocol
 version
IGMP version [71](#)
Independent Basic Service Set
 See IBSS [213](#)
initialization vector (IV) [222](#)
Interface Group [107](#)
Internet Assigned Numbers Authority
 See IANA [182](#)
Internet Group Multicast Protocol [71](#)
IP Address [83, 84, 92](#)
IP alias [82](#)
IP Pool [86](#)

J

Java [118](#)

L

LAN [81](#)
 IP pool setup [82](#)
LAN overview [81](#)
LAN setup [81](#)
LAN TCP/IP [82](#)
Language [148](#)
Link type [34, 41](#)
local (user) database [57](#)
 and encryption [58](#)
Local Area Network [81](#)

M

MAC [62](#)
MAC address [56, 70](#)
 cloning [70](#)
MAC address filter [56](#)
MAC address filtering [62](#)

MAC filter [62](#)
managing the device
 good habits [17](#)
 using the web configurator. See web configurator.
 using the WPS. See WPS.

MBSSID [17](#)

Media access control [62](#)

Memory usage [34, 41](#)

Message Integrity Check (MIC) [221](#)

mode [17](#)

Multicast [71](#)

 IGMP [71](#)

N

NAT [89, 92, 182](#)

 global [90](#)

 how it works [91](#)

 inside [90](#)

 local [90](#)

 outside [90](#)

 overview [89](#)

 see also Network Address Translation
 server [91](#)

NAT Traversal [136](#)

Navigation Panel [35, 42](#)

navigation panel [35, 42](#)

Network Address Translation [89, 92](#)

O

Operating Channel [34, 41](#)

operating mode [17](#)

P

Pairwise Master Key (PMK) [222, 223](#)

Point-to-Point Protocol over Ethernet [75](#)

Pool Size [86](#)

port speed [35, 41](#)

Power Specification [159](#)

PPPoE [75](#)

 dial-up connection

 preamble mode [217](#)

 product registration [234](#)

 PSK [222](#)

Q

Quality of Service (QoS) [65](#)

R

RADIUS [218](#)

 message types [219](#)

 messages [219](#)

 shared secret key [219](#)

RADIUS server [57](#)

registration

 product [234](#)

related documentation [3](#)

Remote management

 and NAT [121](#)

 limitations [121](#)

Reset button [23](#)

Reset the device [23](#)

Restore configuration [148](#)

RF (Radio Frequency) [160](#)

Roaming [63](#)

Router Mode

 status screen [33](#)

RTS (Request To Send) [216](#)

 threshold [215, 216](#)

RTS/CTS Threshold [55, 63, 64](#)

S

safety warnings [6](#)

Scheduling [67](#)

Service and port numbers [115, 135](#)

Service Set [59](#)

Service Set IDentification [59](#)

Service Set IDentity. See SSID.

SSID [34](#), [41](#), [56](#), [59](#)
stateful inspection firewall [111](#)
Static DHCP [87](#)
Static Route [97](#)
Status [33](#)
subnet [175](#)
Subnet Mask [83](#), [84](#)
subnet mask [176](#)
subnetting [178](#)
Summary
 DHCP table [26](#)
 Packet statistics [28](#)
 Wireless station status [28](#)
syntax conventions [4](#)
System General Setup [143](#)
System restart [148](#)

T

TCP/IP configuration [85](#)
Temperature [159](#)
Temporal Key Integrity Protocol (TKIP) [221](#)
Time setting [145](#)

U

Universal Plug and Play [136](#)
 Application [136](#)
 Security issues [136](#)
UPnP [136](#)
URL Keyword Blocking [119](#)
user authentication [57](#)
 local (user) database [57](#)
 RADIUS server [57](#)
User Name [96](#)

V

VLAN operation [101](#)

W

WAN (Wide Area Network) [69](#)
WAN advanced [79](#)
WAN MAC address [70](#)
warranty [233](#)
 note [233](#)
Web Configurator
 how to access [21](#)
 Overview [21](#)
web configurator [17](#)
Web Proxy [118](#)
WEP Encryption [61](#), [62](#)
WEP encryption [60](#)
WEP key [60](#)
Wi-Fi Protected Access [221](#)
Wildcard [95](#)
Wireless association list [28](#)
wireless channel [155](#)
wireless client WPA supplicants [222](#)
wireless LAN [155](#)
wireless LAN scheduling [67](#)
Wireless network
 basic guidelines [55](#)
 channel [56](#)
 encryption [57](#)
 example [55](#)
 MAC address filter [56](#)
 overview [55](#)
 security [56](#)
 SSID [56](#)
Wireless security [56](#)
 overview [56](#)
 type [56](#)
wireless security [155](#), [217](#)
Wireless tutorial [45](#)
WLAN
 interference [215](#)
 security parameters [224](#)
WPA [221](#)
 key caching [222](#)
 pre-authentication [222](#)
 user authentication [222](#)
 vs WPA-PSK [222](#)
 wireless client supplicant [222](#)
 with RADIUS application example [223](#)

- WPA compatible [58](#)
- WPA2 [221](#)
 - user authentication [222](#)
 - vs WPA2-PSK [222](#)
 - wireless client supplicant [222](#)
 - with RADIUS application example [223](#)
- WPA2-Pre-Shared Key [221](#)
- WPA2-PSK [221](#), [222](#)
 - application example [223](#)
- WPA-PSK [221](#), [222](#)
 - application example [223](#)
- WPS [17](#)

